National Nuclear Security Administration

# *Safeguards and Security*

## Qualification Standard
## *Reference Guide*

SEPTEMBER 2006

# Table of Contents

## PURPOSE

The purpose of this reference guide is to provide a document that contains the information required for a National Nuclear Security Administration (NNSA) technical employee to successfully complete the Safeguards and Security Functional Area Qualification Standard. In some cases, information essential to meeting the qualification requirements is provided. Some competency statements require extensive knowledge or skill development. Reproducing all the required information for those statements in this document is not practical. In those instances, references are included to guide the candidate to additional resources.

## SCOPE

This reference guide has been developed to address the competency statements in the December 2003 edition of DOE-STD-1171-2003, Safeguards and Security Functional Area Qualification Standard. Competency statements and supporting knowledge and/or skill statements from the qualification standard are shown in contrasting bold type, while the corresponding information associated with each statement is provided below it. The qualification standard for Safeguards and Security contains 57 competency statements.

Every effort has been made to provide the most current information and references available as of August 2006. However, the candidate is advised to verify the applicability of the information provided.

Please direct your questions or comments related to this document to the Learning and Career Development Department.

## REVISED ORDERS

DOE O 470.4, Safeguards and Security Program, dated August 26, 2005, cancelled the following orders:

DOE O 470.1, Safeguards and Security Program
DOE O 471.2A, Information Security Program
DOE O 471.4, Incidents of Security Concern
DOE O 472.1C, Personnel Security Activities
DOE O 473.1, Physical Protection Program
DOE O 473.2, Protective Force Program
DOE O 474.1A, Control and Accountability of Nuclear Materials

This same Order refers users to the following manuals:

DOE M 470.4-1, Safeguards and Security Planning and Management, August 26, 2005
DOE M 470.4-2, Physical Protection, August 26, 2005
DOE M 470.4-3, Protective Force, August 26, 2005
DOE M 470.4-4, Information Security, August 26, 2005
DOE M 470.4-5, Personnel Security, August 26, 2005
DOE M 470.4-6, Nuclear Material Control and Accountability, August 26, 2005

Current information based on the new documentation has been provided in this reference guide and has been noted as such when applicable.

# TECHNICAL COMPETENCIES

**1. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of physical protection systems.**

**a) Describe the three primary functions of a physical protection system.**

The three primary functions of a physical protection system are detection, delay, and response.

*Detection*

Detection is the discovery of an adversary action that includes sensing covert or overt actions. An effective physical protection system requires that any malevolent act committed must be detected and assessed so that the response can interrupt and neutralize the situation.

*Delay*

Delay is the slowing down of adversary progress. After detection and subsequent assessment, the adversary must be delayed long enough for the response force to arrive and neutralize the situation. The types of delay devices employed can vary from locks, fences, and razor wire to the use of jersey barriers, protective delay barriers, activated delays, spiked vehicle barrier strips, concrete rails, and protective forces (PFs). Whatever means is used, it is critical that it provide additional time to respond to the adversary than what normally would be available without the mechanism(s). Delay time is a variable dependent on the adversary's capabilities and the guard response time, and it varies with the distance between a guard post and the destination to be dispatched, among other factors.

*Response*

Response is defined as the actions taken by the enforcement force — interruption and neutralization — to prevent adversary success. Interruption or interdiction is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress.

**b) Describe the characteristics of an effective physical protection system.**

A well-designed physical protection system (1) provides protection in depth with multiple layers of security that must be defeated in sequence, (2) minimizes the consequences of single component failure, and (3) exhibits balanced protection no matter which path of attack the adversary chooses. Protection can be obtained through various combinations of technology (hardware and software), manpower, and procedures.

Physical protection for each category of special nuclear material (SNM) must consider the following factors: quantities, chemical forms, and isotopic composition purities; ease of separation, accessibility, concealment, and portability; radioactivity; and self-protecting features.

**c) Describe the fundamental characteristics of**

- **Exterior intrusion sensors**
- **Interior intrusion sensors**

Intrusion detection and assessment systems and/or visual observations by PF personnel must be used to protect SNM. Intrusion detection and assessment systems and/or visual observations by authorized personnel must be used to protect classified matter and Government property. When required, intrusion detection and assessment systems must be installed to ensure breaches of security barriers or boundaries are detected and alarms are activated. The systems must be configured so that only authorized personnel may make adjustments.

*Exterior Intrusion Detection System Requirements*

Exterior IDSs are designed to detect unauthorized entry into security areas.

Communication Paths. Exterior IDSs must be designed with independent redundant data communication paths for protecting Category I and II quantities of SNM. The paths must be documented in a Site Safeguards and Security Plan (SSSP) or in a Site Security Plan (SSP).

Detection Capability. A Perimeter Intrusion Detection Assessment System (PIDAS) must be capable of detecting an individual crossing the detection zone by walking, crawling, jumping, running, or rolling, or by climbing the fence at any point in the detection zone, with a detection probability of 90 percent and confidence level of 95 percent.

- The IDS must be tested when installed and annually (at least every 12 months) thereafter to validate that it meets detection probability and confidence level requirements.
- Any time the IDS falls below the required probability of detection, the IDS must be repaired and retested.
- When calculating detection probability for multiple sensor systems, detection is assumed if any of the sensors report an intrusion.

Perimeter Intrusion Detection Assessment System. PIDAS must be

- designed to cover the entire perimeter without a gap in detection, including the sides and tops of buildings situated within;
- located such that the length of each detection zone is consistent with the characteristics of the sensors used in that zone and the topography;
- designed, installed, and maintained to deter adversaries from circumventing the detection system;
- provided with an isolation zone at least 20-feet (6-m) wide and clear of fabricated or natural objects that would interfere with operation of detection systems or the effectiveness of the assessment;
- free of wires, piping, poles, and similar objects that could be used to assist an intruder traversing the isolation zone or that could assist in the undetected ingress or egress of an adversary or matter;
- constructed in a manner that detects and deters the use of wire, piping, pulls, etc., that cannot be eliminated from the isolation zone.

Perimeter Intrusion Detection and Assessment System Zone Degradation. Each PIDAS detection zone must be kept free of snow, ice, grass, weeds, debris, wildlife, and any other item that may degrade the effectiveness of the system. When this cannot be accomplished and detection capabilities become degraded, compensatory measures must be taken.

*Interior Intrusion Detection System (IDS) Requirements*

Interior IDSs are designed to detect unauthorized access to security areas containing classified matter and SNM.

Communication Paths. Interior IDSs must be designed with independent redundant data communication paths for protecting Category I and II quantities of SNM.

Prevention of Bypass. Interior alarm systems must be designed, installed, and maintained to deter adversaries from circumventing the detection system.

- Interior alarms inside material access areas (MAAs) and vault-type rooms (VTRs) must be installed to eliminate gaps in detection coverage.
- The IDS must be tested when installed and annually (at least every 12 months) thereafter.
- If testing indicates degradation of the IDS, it must be repaired and retested.

Unattended Openings. Interior IDSs may be used as compensatory measures for unattended entry/exit points, utility ducts, or other openings.

Balanced Magnetic Switch IDS. Balanced magnetic switches must initiate an alarm upon attempted substitution of an external magnetic field when the switch is in the normal secured position and whenever the leading edge of the door is moved 1 inch (2.5 cm) from the door jamb.

Volumetric Devices. Volumetric interior IDSs must detect an individual moving at a rate of 1 foot per second or faster within the total field of view of the sensor and its plane of detection.

Performance Testing. Interior IDSs must be functionally tested in accordance with locally established procedures at a documented frequency.

**d) Using a list of exterior and interior sensors, describe the classification that should be assigned to each type of sensor.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**e) Describe the types of exterior and interior sensors used within the Department.**

The specific type of sensors used within the Department is considered sensitive information. The following is a general discussion of exterior and interior sensors.

*Interior Intrusion Sensors*

Volumetric sensors monitor an internal area to detect the presence of an intruder. There are several types of volumetric sensors, including microwave, ultrasonic, passive infrared (PIR), and dual-technology (microwave and PIR) sensors. The most commonly used sensors are the dual-technology type.

Dual-technology sensors use both microwave and PIR sensor circuitry within one housing. An alarm condition is generated if either the microwave or PIR sensor generates an alarm condition. In some dual-technology sensors, alarm settings may be adjusted to require that both the microwave and the PIR unit detect an intruder presence before an alarm condition is generated.

Dual-technology sensors have some drawbacks; for example, the PIR channel is relatively vulnerable. An experienced burglar could use an infrared emission-blocking cloak or screen to camouflage his infrared radiation. In addition, in hot climates there can be serious problems with misdetection due to the high ambient temperatures. Some dual-technology sensors attempt to overcome this limitation by having installer-selectable logic, where detectors from either channel are enough to trigger an event. However, this mode is not very popular because it suffers from the false alarm weaknesses of both technologies.

Interior Boundary Penetration Sensors. Boundary penetration sensors detect the presence of an intruder across an interior boundary, such as a door, window, or hatch. Following are the most typical boundary penetration sensors:

- Door switches. The workhorse of the security intrusion detection field, door switches include contact switches, magnetic switches, and balanced magnetic switches. These switches may be used in a variety of applications, from monitoring doors to monitoring hatches, vaults, and panel enclosures. By far, the most effective type is the balanced magnetic switch. This switch has internal circuitry that resists tampering or defeat from strong magnetic fields. By comparison, standard magnetic switches have been defeated by applying a strong magnet to the exterior of the door to bypass an alarm and force the door open.
- Glass-break sensors. There are three basic types of glass-break sensors: acoustic sensors (which listen for an acoustic sound wave that matches the frequency of broken glass), shock sensors (which feel the shock wave when glass is broken), and dual-technology sensors (which detect acoustic and shock vibrations). Because glass-break sensors do not sense motion or intrusion from entering a door or hatch, the sensors should be used in conjunction with other methods (such as volumetric sensors). It is recommended that glass-break sensors not be placed directly on a glass surface.
- Linear-beam sensors. Also referred to as a photoelectric beam or photoelectric eye, a linear-beam sensor consists of a transmitter that emits a beam of light that is invisible to the human eye and a receiver that receives the beam of light. If the beam of light is interrupted or broken by motion from an intruder, an alarm is triggered. Linear-beam detectors can be surface mounted or recessed. These sensors require a straight line of sight between the transmitter and the receiver.

*Exterior Intrusion Detection*

Several types of exterior intrusion detection sensors exist and may be classified according to type, method of use, style, and mode of application. The following exterior systems are most applicable to water system applications and are listed in order from basic to advanced systems in the following paragraphs: freestanding sensors, buried-line sensors, and fence-mounted sensors.

Freestanding Sensors. Freestanding sensors are the most common style of exterior sensor available. Types include active infrared, PIR, microwave, and dual-technology sensors. Microwave and dual-technology detectors are frequently used as freestanding sensors.

Microwave sensors come in two styles: bistatic and monostatic. Bistatic microwave sensors use a transmitter and receiver pair. Monostatic microwave sensors use a single sensing unit that incorporates both transmitting and receiving functions. With both bistatic and monostatic sensors, the sensors operate by radiating a controlled pattern of microwave energy into the protected area. The transmitted microwave signal is received, and a base level no-intrusion signal level is established. Motion by an intruder causes the received signal to be altered, setting off an alarm. Microwave signals pass through concrete and steel and need to be applied with care if roadways or adjacent buildings are near the area of coverage, otherwise nuisance alarms may occur. Many monostatic microwave sensors feature a cut-off circuit, which allows the sensor to be tuned to cover only a selected region to reduce nuisance alarms. Dual-technology sensors use a combination of PIR and microwave technology, as discussed previously.

Buried-Line Sensors. Buried-line sensors include pressure/seismic sensors, magnetic field sensors, buried-ported coaxial cable sensor systems, and buried fiber-optic cable sensor systems. Each of these systems relies on sensing the presence of an intruder by means of a buried cable system within the ground.

One factor that must be considered when using buried-line sensors is the presence of underground utilities. Underground utilities, such as electricity, gas, water, and sewer lines, must be sufficiently below the detection zone, or false alarms may result. Typically, three feet is sufficient to prevent false and nuisance alarms. Rodents are another factor as they have been known to cause maintenance problems by gnawing on the sensor cables. Also, buried-line sensors should not be installed in areas where running water could wash away the soil that buries the sensors, cause nuisance alarms during a heavy rain, or result in standing water or pooling issues.

A drawback to the buried-line sensor system is that it may have different sensitivities when buried below different surfaces. For example, if a continuous system is buried below a concrete surface as well as under a lawn, the sensitivities required for each surface may be different. The sensitivity adjustment required for concrete may be too sensitive for grass. In such a case, it might be best to individually zone those areas so that the sensitivities could be adjusted for each.

Fence-Mounted Sensors. With fence-mounted systems, it is critical that the fence construction be of high quality, with no loose fabric, flexing, or sagging material. The fence should also have solid foundations for posts and gates. Otherwise, nuisance alarms could occur.

Several types of fence-mounted perimeter intrusion detection systems exist. These include electro-mechanical vibration sensing, coaxial strain-sensitive cable, fiber-optic strain-sensitive cable, and taut-wire systems. The two styles of fence-mounted sensors that are most prevalent are coaxial and fiber-optic fence sensing:

- Coaxial strain-sensitive cable systems use a coaxial cable woven through the fabric of the fence. The coaxial cable transmits a dielectric field. As the cable moves due to strain on the fence fabric caused by climbing or cutting, the electric field changes are detected within the cable, and an alarm condition occurs. Coaxial strain-sensing systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. Some coaxial cable systems are susceptible to electromagnetic interference and radio frequency interference.
- Fiber-optic strain-sensitive cable systems are similar to the coaxial strain-sensitive cable systems. The fiber-optic system uses a fiber-optic cable, rather than a coaxial cable, woven through the fence fabric. Strain on the fence fabric causes micro-bending of the fiber cable, which is monitored by the control panel and generates an alarm condition. Fiber-optic strain-sensing systems are relatively new detection systems, but have a strong following. The systems are readily available and are highly tunable to adjust for field conditions due to weather and climate characteristics. The systems are impervious to lightning, electromagnetic interference, radio frequency interference, or other electronic signals, and can be used over long distances.

Possible defeat measures of fence-mounted systems include tunneling, jumping, or bridging across the fence system. Careful climbing at corner posts also may not generate sufficient vibration to generate an alarm condition.

**f) Describe the components of a comprehensive entry control system.**

Access control systems and entry control points must provide positive control that allows the movement of authorized personnel, vehicles, packages, and hand-carried items along normal routes, while detecting and delaying entry of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of safeguard and security interests.

Entry control point design must incorporate the following:

- Entry control points for vehicle and pedestrian access to security areas must provide the same level of protection as that provided at all other points along the security perimeter.
- Entry control points must be structurally hardened to meet site-specific criteria.
- Exits from security areas must satisfy the life safety requirements of National Fire Protection Association (NFPA) 101, Safety to Life from Fire in Buildings and Structures. Some exits may be provided for emergency use only.
- Entrances to and exits from security areas must be equipped with doors, gates, rails, or other movable barriers that direct and control the movement of personnel or vehicles through designated control points.
- Door locks and latches used on security area perimeters must meet the requirements of NFPA 101.
- Motorized gate controls, where used, must be located within PF posts at entry control points. Motorized gates must be designed to allow manual operation.
- Entry control points must facilitate ingress and egress of emergency vehicles and fire protection equipment.
- The number of entry control points for each security area must be limited to maintain barrier integrity.

- Entry control points must be located within the PIDAS and protected by the PIDAS when not in use. This configuration must provide a continuous PIDAS zone at the barrier that encompasses the entry control point.

**g) Describe the types of entry control systems used within the Department.**

Many DOE facilities are guarded by a sophisticated, computerized security system called Argus. Argus was designed, engineered, and installed at the Lawrence Livermore National Laboratory (LLNL) and is continually being upgraded and enhanced. It is also available to other DOE and U.S. Department of Defense (DOD) facilities.

Although named for the hundred-eyed monster of Greek mythology, Argus security comprises much more than visual capabilities. A highly interconnected network engineered with comprehensive security features, Argus lives up to such stringent security requirements that DOE's Office of Safeguards and Security has cited it as the standard for physical security systems protecting facilities where the consequences of intrusion are significant. In addition to LLNL, the Argus system has been installed at three other DOE sites and at one DOD site to protect top-priority assets or nuclear material.

As it monitors and controls entry into the LLNL high-security buildings, Argus is simultaneously monitoring the entire site for security threats and can alert and direct security forces to those threats. Argus security is all-encompassing and omnipresent, but it is surprisingly noninvasive. Employees of LLNL enter and move about the laboratory campus with relative ease, yet the laboratory's top secret documents, materials, and facilities are thoroughly protected, intruders can be detected in real time, and intrusions and emergencies get instantaneous response from police and investigative personnel. The laboratory is provided with maximum security 24 hours a day, 7 days a week.

This security results from a software system that comprises some 1.5 million lines of code, offering a wide range of security features. Extensive features are necessary, because Argus must accommodate many different configurations of security rules within one security complex, and sometimes one complex may have multiple geographic locations (for example, LLNL's Argus system controls the main site and the nearby Site 300 high-explosives testing facility). Moreover, Argus must be reconfigurable at any time. Extensive features also translate into flexibility and simplicity for end users. That is important because every authorized person in a high-security site accesses and interfaces with the Argus system. To ensure that designers, operators, and users understand Argus, DOE's National Training Center in Albuquerque, New Mexico, has 14 classes available, ranging in length from one hour to one week, that cover the complete set of Argus features.

While protecting a security complex, Argus also protects itself. A high degree of redundancy has been incorporated to prevent system failure, and tamper-indicating devices and data encryption have been used throughout to protect surveillance equipment and data from intruders and thieves. Insider threats to weaken the system have been addressed with a comprehensive set of system-enforced and procedural measures, including consistency checking, captive accounts, and a rule prohibiting people from working alone.

**h) Describe the purpose of access delay in a physical protection system.**

Delay mechanisms must be used to deter and delay access, removal, or unauthorized use of Category I and II quantities of SNM and nuclear weapons. Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, and cold smoke). Active and/or passive denial systems must be used at site-specified target locations, as appropriate, to reduce reliance on PF recapture/recovery operations.

Permanent physical barriers must identify the boundary of a security area and must be capable of controlling, impeding, or denying access to a security area. Barriers are used to: direct the flow of personnel and vehicles through designated entry control points; delay and/or deter the introduction of prohibited and controlled articles or the removal of safeguards and security (S&S) interests; delay and/or prevent penetration of a security area by vehicles; and channel personnel and vehicles along designated target area pathways to extend the ability of PF personnel to identify and engage armed adversaries.

**i) Describe the type of access delay mechanisms used within the Department.**

Delay mechanisms may include both passive physical barriers (e.g., walls, ceilings, floors, windows, doors, and security bars) and activated barriers (e.g., sticky foam, pop-up barriers, and cold smoke).

**j) Discuss the following terms:**
- **Probability of detection**
- **Delay time**

*Probability of Detection*

Probability of detection is the likelihood of a detection element of a physical security system (e.g., sensor, security police officer, etc.) to recognize an external stimulus as an adversarial action within a specific zone of coverage.

*Delay Time*

Delay is the slowing down of adversary progress. After detection and subsequent assessment, the adversary must be delayed long enough for the response force to arrive and neutralize the situation. The types of delay devices employed can vary from the locks, fences, and razor wire to the use of jersey barriers, protective delay barriers, activated delays, spiked vehicle barrier strips, concrete rails, and PFs. Whatever means is used, it is critical that it provide additional time to respond to the adversary than what normally would be available without the mechanism(s). Delay time is a variable dependent on the adversary's capabilities and the guard response time, and it varies with the distance between a guard post and the destination to be dispatched, among other factors.

**k) Demonstrate the modeling of a physical protection system using an adversary sequence diagram.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**2. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of protective force operation.**

**a) Describe the levels and associated responsibilities of protective force personnel within the Department of Energy (DOE).**

*Security Officers (SOs)*

Responsibilities. Where practicable, unarmed SOs should be used to perform administrative, access control, facility patrol, escort, alarm assessment, alarm monitoring, and dispatch duties, as well as reporting of alarms. SOs will enforce S&S protection requirements allowing armed PF personnel to maintain focus on their primary mission of combating the armed terrorist threat. Where possible, technological means (e.g., automated access controls, passive and active barriers, etc.) will be used to reduce staffing requirements.

*Security Police Officers (SPOs)*

Responsibilities. Title 10 Code of Federal Regulations (CFR) 1047, Limited Arrest Authority and Use of Force by PF officers, delineates the SPOs' responsibilities at DOE facilities (other than the Strategic Petroleum Reserve [SPR]) to enforce specified laws regarding Government property and criminal provisions of the Atomic Energy Act. Such SPOs may, in accordance with 10 CFR 1047, be given additional local law enforcement responsibility on a site-specific basis. Title 10 CFR 1049, Limited Arrest Authority and Use of Force by PF officers of the SPR, delineates SPO responsibility at the SPR to enforce Federal criminal laws to protect SPR Government property and personnel. SPOs must possess the individual and team combat tactical skills necessary to protect S&S interests from an armed terrorist threat, to include theft or sabotage of nuclear weapons or special nuclear material, and other hostile acts that may cause adverse impacts on national security, the health and safety of employees, the public, or the environment.

Armed SPOs must be assigned to protect security areas that

- receive, use, process, or store Category I or II quantities of SNM;
- manufacture, store, or test nuclear weapons, nuclear test devices, or complete nuclear assemblies;
- represent a significant target for sabotage (e.g., they are radiological or toxicological);
- contain a unique capability in DOE that must be protected for purposes of program continuity or to preclude an unacceptable impact to national security, the health and safety of DOE and contractor employees, the public, or the environment when the need has been so designated by the DOE line management.

SPOs are categorized according to a three-level system (SPO-I, SPO-II, and SPO-III) that tailors training requirements to assigned duties.

| SPO Level | Response Category | Assignments |
|---|---|---|
| SPO-I | Static defense | ▪ Category I/II facilities — Fixed fighting positions, towers, access control, alarm monitoring, dispatch, security checks, armed construction/administrative escort, and material/package inspections<br>▪ Non-Category I/II facilities — Vehicle and foot patrols, alarm response and assessment, access control, alarm monitoring, dispatch, security checks, armed construction/administrative escort, and material/package inspections |
| SPO-II | Active defense | ▪ Vehicle and foot patrols<br>▪ Mobile and mobile reserve response force with the primary mission of denying adversary access to targets |
| SPO-III | Active defense | ▪ Exterior reconnaissance patrols and special response team (SRT) posts<br>▪ Activities and duties with the primary missions of recapture, recovery, and pursuit |

*Federal Agents (FAs)*

Responsibilities. Armed DOE PF personnel designated as FAs under the authority of the Assistant Deputy Administrator for Secure Transportation must provide for the safe, secure, off-site domestic transportation of the following:

- DOE-owned or DOE-controlled nuclear explosives and nuclear devices
- Category II or greater quantities of SNM, excluding naval reactor core shipments
- limited-life components of nuclear weapons
- other materials approved by the Assistant Deputy Administrator for Secure Transportation

*Federal Officers (FOs)*

Responsibilities. DOE Federal employees that are designated as FOs by the Director, Office of Security, or the DOE cognizant security authority, may or may not possess firearms/arrest authority pursuant to section 161.k. of the Atomic Energy Act or section 661 of the DOE Organization Act, and must, when directed

- conduct investigations
- conduct liaison activities with law enforcement officials
- perform inquiries into local and national security issues

*Special Agents (SAs)*

Responsibilities. Armed DOE Federal employees that are designated as SAs by the Director, Office of Security, possess firearms/arrest authority pursuant to section 161.k. of the Atomic Energy Act or Section 661 of the DOE Organization Act, may be deputized by the U.S. Marshals Service, and must, when directed

- participate in special operations such as executive protection
- conduct investigations
- conduct liaison activities with law enforcement officials
- perform inquiries into local and national security issues

**b) Describe the role of a special response team.**

The mission of the SRT is to resolve incidents that require force options that exceed the capability of SPO-I and SPO-II personnel and/or existing physical security systems. The SRT must be capable of effective and ready response. The SRT must be trained and equipped to conduct interdiction, interruption, and neutralization operations, as well as containment, denial, recapture, recovery, and pursuit strategies directed against an adversary.

An SRT is required at facilities or sites that receive, use, transport, or process Category I quantities of SNM (including a credible roll-up of Category II to Category I quantities of SNM). The authorization for an SRT capability at a Departmental site or facility not meeting these requirements must be approved by DOE line management, with notification to the cognizant Departmental element. Approvals must be based on a site Vulnerability Assessment (VA) that documents the need for an SRT (e.g., a radiological/toxicological/ sabotage target that could have adverse impact on national security, the health and safety of employees, the public, or the environment).

The SRT must be staffed with qualified and certified SPO-III personnel deployed as one or more dedicated teams with specialized weapons and equipment, operating from mobile tactical vehicles, as ground assault forces, or a combination of both.

**c) Discuss the following terms:**

- **Interdiction**
- **Interruption**
- **Neutralization**
- **Recapture**
- **Denial**

*Interdiction*

Interdiction is the act of stopping or delaying an adversary before he/she reaches or achieves his/her objective.

*Interruption*

Interruption is the disruption of an adversarial activity before it reaches or achieves its objective.

*Neutralization*

Neutralization means to counteract the activity or effect of an adversary.

*Recapture*

Recapture means to regain control of a nuclear weapon and/or special nuclear material that is under unauthorized possession while still within the confines of a Departmental site/facility.

*Denial*

Denial is the effect achieved by S&S systems or devices that prevents a potential intruder or adversary from gaining access to, or use of, a particular space, structure, facility, or asset.

**d) Describe typical examples of Federal or state authority granted to Protective Force personnel.**

*Coordination with Other Law Enforcement Authorities*

When other federal, state, or local law enforcement authorities with jurisdiction in the area into which the suspected criminal has fled join the pursuit, they must be primarily responsible for the continued pursuit.

The PF dispatcher, supervisors in the PF command structure, and the officer in charge of on-site PF operations must coordinate the pursuit efforts of PF officers with other federal, state, and/or other local law enforcement authorities who assume primary responsibility.

PF officers participating in the pursuit must continue to participate in pursuit operations until otherwise instructed by the PF dispatcher, respective supervisors in the PF command structure, or the officer in charge of on-site PF operations.

At least one PF officer unit will remain available to assist the other pursuing federal, state, and/or other local law enforcement authorities until the pursuit is concluded or otherwise terminated. That PF officer will thereafter provide such law enforcement authorities with all relevant information regarding the circumstances surrounding the incident.

*Arrests*

When other federal law enforcement authorities (e.g., the Federal Bureau of Investigation [FBI] or a U.S. Marshal) are involved with PF officers in the apprehension of a suspected criminal (regardless of whether on or off DOE property), PF officers must relinquish arresting authority to the other federal law enforcement authorities.

When state or other local law enforcement authorities are involved with PF officers in the off-site apprehension of a suspected criminal, the issue of which law enforcement official is in charge in order to effect an arrest is generally not a matter of policy but one of common sense dictated by the circumstances. Such an assessment includes an evaluation of the expertise of those present, which agency has first established control, and the disruptive effect, if any, of transfer of control. The determination of which jurisdiction should make the arrest is, therefore, left to the discretion of the officers involved. To the extent practicable, guidelines addressing this issue should be prepared on a site-by-site basis in coordination with State and other local law enforcement authorities. Such guidelines must be included in the site-specific guidelines submitted to the Director, Office of Security, for approval.

When a suspected felon is apprehended (regardless of whether on or off DOE property), or when a suspected misdemeanant is apprehended on DOE property, the PF must immediately notify the appropriate U.S. Attorney's Office and escort the suspect to the nearest U.S. District Court or U.S. Magistrate for arraignment (unless otherwise directed by local Federal law enforcement authorities, e.g., the FBI or a U.S. Marshal). Under no circumstances should a suspected felon be removed to another jurisdiction without first being processed through the federal criminal justice system where the suspected felon was apprehended.

The pursuing PF officers must ensure that any Government property retrieved during pursuit or at the time of apprehension is properly secured and a chain of custody is established.

**3. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of protection program operations as described in DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, and DOE M 471.2-1, Classified Matter Protection and Control Manual.**

Note: DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, DOE M5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, and DOE M 471.2-1, Classified Matter Protection and Control Manual have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-2, Physical Protection, DOE M 470.4-4, Information Security, and DOE M 470.4-7, Safeguards and Security Program References.

**a) Describe the five elements of protection and control planning:**

- **Site-specific characteristics**
- **Threat**
- **Protection strategy**
- **Planning**
- **Graded protection**

*Site-Specific Characteristics*

Protection programs must be tailored to address specific site characteristics and requirements, current technology, ongoing programs, and operational needs to achieve acceptable protection levels that reduce risks in a cost-effective manner.

*Threat*

A threat is defined as

- a person, group, or movement with intentions to use extant or attainable capabilities to undertake malevolent actions against Departmental interests;
- the capability of an adversary coupled with his/her intentions to undertake any actions detrimental to the success of program activities or operations;
- any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.

*Protection Strategy*

A protection strategy is comprised of technical and tactical techniques to mitigate the design basis threats (DBTs) against special nuclear material, vital equipment, classified matter, and other Departmental property. The strategies are for the protection of Departmental property from adversary actions that would impact national security, the health and safety of employees, the public, or the environment.

*Planning*

Planning must be integrated with other programs such as physical protection, PF, information security, personnel security, and material control and accountability (MC&A). Mechanisms must also exist to assure that S&S program planning is fully integrated with overall site

strategic and near-term operational planning. S&S plans must be developed for facilities with any of the following S&S interests:

- Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity
- Category II, Category III, or Category IV SNM
- Radiological, chemical, or biological sabotage threats
- Critical mission disruption threats
- Intra-/inter-site transportation of SNM
- Classified information or matter
- Facilities engaged in the protection of Government property
- Facilities that the Secretary, Deputy Secretary, or Under Secretaries deem appropriate

*Graded Protection*

Graded protection is defined as the policies and S&S measures (level of effort and resources) that are applied in a proportional manner toward the protection of S&S interests based on the impact of their loss, destruction, or misuse.

**b) Describe how the design basis threat is used in safeguards and security program planning.**

DOE O 470.3, Design Basis Threat Policy (U), must be used with local threat guidance during the conduct of VAs for protection and control program planning. The DBT must be the baseline threat definition, but local threat guidance may be used to increase the level of threat to be analyzed.

Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and specific threat indicators. Threat indicators should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of threat indicators that can be used to develop a site-/facility-specific assessment are listed below:

- International incidents or indicators against U.S. interests, personnel, or facilities
- Domestic incidents or indicators against federal or state interests countrywide
- Local incidents or indicators directed against federal or DOE interests
- Specific targeting of DOE personnel, facilities, or materials

Note: DOE O 470.3, Design Basis Threat Policy (U), is a classified order and must be requested through DOE Headquarters.

**c) Describe the method used to identify and characterize the range of potential adversary threats.**

Critical path scenarios are used to identify and characterize the range of potential adversary threats. Critical path scenarios, including the bounding scenarios, are developed during the VA for each target, and the protection system effectiveness is identified for each of these targets. Critical detection points along each adversary path are also described and identified.

**d) Discuss the denial strategy used to protect safeguards and security interests.**

Denial is the effect achieved by S&S systems or devices that prevents a potential intruder or adversary from gaining access to or use of a particular space, structure, facility, or asset. The basic strategies pertaining to protection are denial of access, denial of task, and containment, which upon failure could evolve into recapture/recovery or pursuit strategies. For denial-based protection systems, the point on the pathway is the critical detection point. The critical detection point is defined as the point at which the PF must have timely detection, assessment, and response in order to initiate a response with a high probability of success in the neutralization of the adversary or denial of the adversary's task/objective. Therefore, for a facility employing multiple, complementary layers of protection, the representative total protection system effectiveness is calculated up to the point at which the protection systems can still effectively engage an adversary prior to completion of the objective.

*Denial Strategy Implementation*

The following actions are part of denial strategy implementation:

- Early warning system technologies are emplaced to detect and to assess adversary movement as far as possible from target locations.
- Highly mobile tactical vehicles (armored and/or unarmored) mounted with light and/or heavy weapon systems are deployed to support combat operations, conduct reconnaissance operations, control avenues of approach, maneuver to suppress and destroy hostile threats, and to provide mutual support for other tactical vehicles.
- A commander is designated for each tactical armored vehicle (for a two-person crew, usually the gunner).
- Potential target access points are covered by suppressive fire weapons.
- Tactical Response Force (TRF) members utilize positions of cover and maximize the element of surprise to the extent possible.
- The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.
- Once an adversary has been identified and engaged, TRF elements never lose contact.
- Adversaries are engaged while they negotiate obstacles (i.e., fences, barriers, etc.), deploy from vehicles (both airborne and ground based), and cross open ground.
- TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.
- The TRF has plans in place to transition quickly from defensive to offensive operations.

**e) Describe the containment strategy for Category I and II special nuclear material.**

Containment is the effect achieved by S&S systems and personnel that prevents an adversary or SNM from leaving a particular space, structure, or facility.

**f) Discuss the recapture/recovery or pursuit strategy should containment fail.**

The site PF is staffed and deployed in sufficient strength to ensure the protection of sensitive assets. The dedicated recapture/recovery element of the SRT is established with additional resources sufficient to ensure that recapture/recovery capabilities continue to exist in the event that the denial strategy fails.

SRT training is focused on site-specific targets and ensures that SRTs are adequately prepared to conduct recapture/recovery operations within identified target locations. SRTs possess the tactics, tools, and techniques necessary to gain entry, neutralize the adversary threat, control the situation, and secure national security assets. If hostages are involved and SNM is at risk, regaining control of the SNM is the primary consideration.

SRTs are supported by other TRF elements to the maximum extent possible as they move toward the target objective. TRF members provide overwatch for the assault team(s) movement, cover avenues of approach, and provide support by fire to the SRT as they breach/enter the target location. All TRF personnel are capable of providing direct support to the recapture/recovery mission by supplementing the main assault force, controlling the target area, and suppressing enemy defensive positions.

**g) Discuss the programs designed to mitigate radiological/toxicological sabotage.**

*Radiological, Chemical, or Biological Sabotage*

Physical protection strategies must be developed, documented, and implemented consistent with the DBT to protect radiological, chemical, or biological sabotage targets:

- Radiological Sabotage. Targets must be protected in a graded manner to protect S&S interests and to mitigate consequences of a radiological sabotage event.
- Chemical and Biological Sabotage. Targets must be protected to protect S&S interests and to mitigate consequences of a chemical or biological sabotage event.

*Mitigation*

The implementation of the following prevention and mitigation measures must be based on the results of the radiological, chemical, or biological sabotage analysis:

- S&S features to detect or delay adversary actions (i.e., access and materials controls, surveillance, additional barriers/alarms, and entry/exit inspections)
- additional controls or equipment that would prevent a sabotage release scenario (e.g., providing automatic shutdown if components fail, adding backup systems, or establishing security areas)
- event-mitigating actions such as establishing shelters, emergency notifications/evacuations, reducing and/or removing inventory quantities, or changing storage locations

**h) Describe the methods for protection and control of classified matter.**

The following are general requirements for the protection of classified information or matter:

- Classified information or matter is any combination of documents and material containing classified information. This includes classified parts and explosives whose shapes are considered classified.
- Classified matter must be processed, handled, or stored in security areas that provide protection measures equal to or greater than those present in a Limited Area (LA).
- Classification levels must be used in determining the degree of protection and control required for classified matter. Custodians and authorized users of classified matter are responsible for the protection and control of such matter.
- Access to classified matter must be limited to persons who possess appropriate access authorization and require such access ("need to know") in the performance of official duties. Controls must be established to detect and deter unauthorized access to classified matter.

- Buildings and rooms containing classified matter must have the security measures necessary to deter unauthorized persons from gaining access to classified matter. This includes security measures to deter persons outside the facility protective zone from viewing or hearing classified information. Conference rooms and areas specifically designated for classified discussions must follow the Technical Surveillance Countermeasures program requirements.

**i) Describe the requirements for the protection of unclassified irradiated reactor fuel while it is in transit.**

Physical protection for each category of SNM must consider the following factors: quantities, chemical forms, and isotopic composition purities; ease of separation, accessibility, concealment, and portability; radioactivity; and self-protecting features. The protection of nuclear material production, reactors, and fuel must be commensurate with the category of SNM.

**j) Discuss the graded approach in relation to the protection of safeguards and security interests.**

The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for, or consequences of, all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

**k) Discuss the requirements of the following protection elements:**
- **Intrusion detection and assessment systems**
- **Access control and entry/exit inspections**
- **Barriers and locks**
- **Secure storage**
- **Communications**
- **Acceptance and validation testing**
- **Maintenance**
- **Posting notices**
- **Security badges and credentials**

*Intrusion Detection and Assessment Systems*

Intrusion detection and assessment systems and/or visual observations by PF personnel must be used to protect SNM. Intrusion detection and assessment systems and/or visual observations by authorized personnel must be used to protect classified matter and Government property. When required, intrusion detection and assessment systems must be installed to ensure breaches of security barriers or boundaries are detected and alarms are activated. The systems must be configured so that only authorized personnel may make adjustments.

*Access Control*

Access must be based on an individual's "need to know" to perform official duties, validation of the individual's access authorization, and the presentation of a DOE security badge. A person

allowed to enter an LA, exclusion area (EA), protected area (PA), vital area, or MAA without an appropriate access authorization must be escorted at all times by an individual with

- knowledge of security procedures for the security areas to prevent compromise of classified information or matter
- appropriate access authorization
- "need to know" for the security area or the S&S interests

*Entry/Exit Inspections*

Entry inspections of personnel, hand-carried items, packages, and/or vehicles must ensure prohibited articles are detected and are not introduced without authorization. Exit inspections must ensure S&S interests are not removed without authorization.

*Barriers*

Permanent physical barriers must identify the boundary of a security area and must be capable of controlling, impeding, or denying access to a security area. Barriers are used to direct the flow of personnel and vehicles through designated entry control points; delay and/or deter the introduction of prohibited and controlled articles or the removal of S&S interests; delay and/or prevent penetration of a security area by vehicles; and channel personnel and vehicles along designated target area pathways to extend the ability of PF personnel to identify and engage armed adversaries.

*Locks*

All security containers placed into service after July 14, 1994, must have a lock that meets Federal Specification FF-L-2740A.

*Secure Storage*

S&S interests requiring secure storage must be placed in vaults, VTRs, VTR complexes, and/or General Services Administration-approved security containers. A vault and/or VTR or security container must be located within an LA.

*Communications*

Communications equipment must be provided to facilitate reliable information exchanges between protective personnel. Voice communications systems used for security purposes must provide intelligible voice communications in all security areas for all modes of operation and operating conditions. Security system transmission lines and data must be protected in a graded manner from tampering and substitution. The communications equipment must meet the following requirements.

- Redundant Voice Communications. Facilities protecting Category I and II quantities of SNM must have a minimum of two different voice communications technologies to link the Central Alarm Station (CAS)/Secondary Alarm Station (SAS) to each fixed post and PF duty location. Alternative communications capabilities must be available immediately if the primary communications system fails. Channels considered critical to protective personnel communications must have backup stations. Records of the failure and repair of all communications equipment must be maintained so that type of failure, unit serial number, and equipment type can be compiled.

- Recording of Communication. A continuous electronic recording system must be provided for all security radio traffic and telecommunications lines that provide support to the CAS. The recorder must be equipped with a time track and must cover all security channels. This recording requires the approval of the Office of the Chief Information Officer and the Office of Security or the Office of the Associate Administrator for Defense Nuclear Security.
- Loss of Primary Power. Systems must remain operable during the loss and recovery of primary electrical power.

*Acceptance and Validation Testing*

Information on acceptance and validation testing was not available.

*Maintenance*

Security-related subsystems and components must be maintained in operable condition. A regularly scheduled testing and maintenance program must be established and documented.

Corrective Maintenance. Corrective maintenance must be performed on site-determined critical and noncritical physical protection system elements:

- Compensatory Measures. Compensatory measures must be implemented immediately when any part of the critical system element protecting Category I and II quantities of SNM, vital equipment, and Top Secret matter is out of service. Compensatory measures must be continued until maintenance is complete and the critical system element is back in service. For noncritical system elements, the cognizant security authority must approve compensatory measure implementation procedures.
- Corrective Maintenance within 24 Hours. Corrective maintenance must be initiated within 24 hours of indication that there has been a malfunction of a site-determined critical system element protecting Category I and II quantities of SNM, vital equipment, or Top Secret matter.
- Corrective Maintenance within 72 Hours. Corrective maintenance must be initiated within 72 hours of detection of a malfunction for all other protection system elements protecting Category I and II SNM, vital equipment, or Top Secret matter.
- Other Corrective Maintenance. Corrective maintenance procedures for protecting Category III and IV quantities of SNM or Secret or Confidential matter must be approved by line management and prescribed in the site's operation procedures.

Preventative Maintenance. Preventive maintenance must be performed on critical S&S-related subsystems and components. Preventive maintenance must comply with the manufacturer's specifications and recommendations.

Critical Component Preventive Maintenance. The following system elements must be included in a preventive maintenance program:

- Intrusion detection and assessment systems
- CAS and SAS communications and display systems
- Data and voice communications systems
- PF equipment
- Access control and entry/exit inspection equipment

- Package and hand-carried items inspection equipment
- Vehicle access control and inspection equipment
- Security and safety lighting systems

Other Preventive Maintenance. PIDAS, security area and other security lighting, and security system-related emergency power or auxiliary power supplies must be included in a preventive maintenance program.

*Posting Notices*

Signs must be posted at facilities, installations, and real property based on the need to implement federal statutes protecting against degradation of S&S interests. Signs listing prohibited and controlled articles must be posted at security area entrances. Warning signs and/or notices must be posted at entrances to areas under electronic surveillance advising that physical protection surveillance equipment is in operation.

*Security Badges and Credentials*

DOE security badges must be issued to and worn by all DOE and contractor personnel to gain access to DOE facilities with S&S interests and security areas. DOE security badges or Office of Science (SC) badges are the only formats to be used:

- DOE Security Badge. The following requirements apply:
  - Specifications for the DOE security badge and Local Site-Specific Only badge are identified in M470.4-2, Appendix 1.
  - The DOE security badge will be accepted at all Departmental facilities. Individuals at SC facilities with an access authorization must be issued a DOE security badge to gain access to non-SC Departmental facilities.
  - Employee identification cards must not be substituted for the DOE security badge or the SC badge.
  - The SC badge is not authorized for access to Departmental facilities that require the DOE security badge.
- Office of Science Badge. SC must prepare and distribute specifications for the badge. DOE line management must approve locally developed procedures for the issuance, use, recovery, accountability, protection, and destruction of the SC badge that are documented in the security plan. Facilities operated exclusively by SC, Office of Fossil Energy, and the Office of Energy Efficiency and Renewable Energy that use the SC badge are exempted from the DOE security badge requirements.

**4. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of the protection of special nuclear material as described in DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M 5632.1C - 1, Manual for Protection and Control of Safeguards and Security Interests.**

Note: DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, and DOE M 470.4-2, Physical Protection.

**a) Describe access procedures to storage repositories.**

Access to vaults and VTR must be strictly controlled and based on an appropriate access authorization and "need to know."

- Persons without "need to know" and the appropriate access authorization must be escorted at all times.
- Protective measures to mask classified matter must be used before visitors or cleared persons without "need to know" receive access.
- Means of controlling access must be documented in an SSSP or an SSP.
- Access controls at vaults and VTR must provide logging or recording of all personnel entries and exits, including visitors. Logged or recorded entries must include the identification/name and date/time of entry and exit.
  - In vaults and VTR where entering personnel are restricted from access (e.g., a foyer) to classified matter or SNM, logging entry and exit is not required.
  - The cognizant security authority may waive the requirement for repeated logging for those personnel whose offices are located within the boundary of the vaults and vault-type rooms. Initial daily entry and final daily exit logging are required.

**b) Describe procedures to prevent and detect unauthorized access to a storage repository.**

Interior IDSs are designed to detect unauthorized access to security areas containing classified matter and SNM. Barriers such as fences, walls, and doors, or activated barriers, must be used to deter and delay unauthorized access. Doors or openings allowing access into vaults must be equipped with IDS devices. A balanced magnetic switch or other equally effective device must be used on each door or movable opening to allow detection of attempted or actual unauthorized access.

**c) Describe the procedures for investigating and reporting abnormal conditions.**

Incidents of security concern are actions, inactions, or events that have occurred at a site that

- pose threats to national security interests and/or critical DOE assets
- create potentially serious or dangerous security situations
- potentially endanger the health and safety of the workforce or public (excluding safety-related items)
- degrade the effectiveness of the S&S program
- adversely impact the ability of organizations to protect DOE S&S interests

Incidents of security concern must be categorized in accordance with their potential to cause serious damage or place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, PF, information security, personnel security, and nuclear MC&A. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

*Reporting Requirements*

The 24-Hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens) must be sent to the DOE Headquarters (HQ) Operations Center (OC) using DOE Form (F) 471.1, "Security Incident Notification Report," in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria:

- Within one hour following categorization for security incidents determined to be IMI-1, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.
- Within eight hours following categorization of security incidents determined to be IMI-2/IMI-3, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within eight hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1 and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the Office of Counterintelligence/Office of Defense Nuclear Counterintelligence must be notified.

Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the Sensitive Compartmented Information (SCI) Program, the Special Access Program (SAP), the Technical Surveillance Countermeasures (TSCM) Program, the Counterintelligence (CI) Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report must be transmitted to the Office of Security for entry into the Incident Tracking and Analysis Capability database.

*Final Inquiry Reports*

Inquiry officials must forward final inquiry reports in accordance with local procedures to line management for action and to the Office of Security.

*Inquiry Officials*

The following requirements apply to inquiry officials:

- Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.
- Inquiry officials may be either federal or contractor employees, but must have previous investigative experience or Department inquiry training and must be knowledgeable of appropriate laws, Executive orders, Departmental directives, and/or regulatory requirements.
- Inquiry officials are not authorized to detain individuals for interviews or to obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.
- Inquiry officials must be appointed in writing by DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.
- Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).
- When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

*Conduct of Inquiries*

If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry:

- If the sites/facilities fall under the purview of a single DOE cognizant security authority, that DOE cognizant security authority must assign responsibility to a lead organization.
- If the sites/facilities fall under the purview of multiple DOE cognizant security authorities, those DOE cognizant security authorities must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

When conducting inquiries into incidents of security concern, the following actions must be taken and reflected in the inquiry report:

- Data Collection.
  - Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
  - Conduct interviews to obtain additional information regarding the incident.
  - Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment.)
  - Ensure physical evidence is protected and controlled and a chain of custody is maintained.
- Incident Reconstruction.
  - Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
  - Develop a chronological sequence of events that describes the actions preceding and following the incident.
  - Identify persons associated with the incident.

- Incident Analysis and Evaluation. This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must perform the following tasks:
  - Analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately.
  - Collect additional data and reconstruct the incident if more information is required.
  - Identify any collateral impact with other programs or security interests.

In addition, inquiry officials must perform the following actions:

- Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.
- Ensure a DOE F 5639.2, Reporting Unaccounted for Documents, or a form comparable in content, is completed if classified information or matter is missing.
- Determine which Departmental element has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.
- Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).
- If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.
- When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the Department of Justice (DOJ) Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.
  - Could the date and identity of the article or articles disclosing the classified information be provided?
  - Could specific statements in the article that are considered classified be identified? Was the data properly classified?
  - Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.
  - Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?
  - Could the extent and official dissemination of the data be determined?
  - Has it been determined that the data has not been officially released in the past?
  - Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?

- Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?
- Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.
- Has it been determined that declassification had not been accomplished prior to the publication or release of the data?
- Will disclosure of the classified data have an adverse impact on the national defense?

**d) Describe the protective responsibilities when special nuclear material is out of the vault.**

The following requirements apply when SNM is out of the vault:

- Category I quantities of SNM must be located within an MAA inside a PA. Any MAA containing unattended Category I quantities of SNM must be equipped with an IDS or other means of detection approved by the cognizant DOE line management.
- Category II quantities of SNM must be located within a PA and under material surveillance procedures.
- Category III quantities of SNM must be used or processed within an LA.
- Category IV quantities of SNM must be used or processed within at least a property protection area (PPA) and in accordance with local security procedures approved by DOE line management.

**e) Describe the protective responsibilities when special nuclear material is in transit.**

*CAT I and II Quantities of SNM*

The following requirements apply to transportation of CAT I and II quantities of SNM:

- Domestic off-site SNM shipments must be made by the Office of Secure Transportation (OST).
- Packages or containers containing the SNM must be sealed with tamper-indicating devices.
- Protection measures for movements of the SNM, between PAs at the same site or between PAs and staging areas on the same site, must be under constant surveillance by armed PF escorts.

*Cat III Quantities of SNM*

Category III quantities of SNM may be transported by the following methods unless otherwise prohibited by statute:

- Domestic off-site shipments of classified configurations of Category III quantities of SNM must be made by the OST.
- Off-site shipments of unclassified configurations of Category III quantities of SNM are not required to be made by OST. If OST is not used, such shipments may be transported by the following authorized methods:
  - Truck or train shipment
  - Air Shipment (Shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.)
- Movement between security areas at the same site must comply with the locally developed shipment security plan.

*CAT IV Quantities of SNM*

Category IV quantities of SNM may be transported by the following methods unless otherwise prohibited by statute:

- Domestic off-site shipments of classified configurations of Category IV quantities of SNM may be made by the OST or by other means when approved by DOE line management.
- Shipments of unclassified Category IV quantities of SNM may be made by truck, rail, air, or water craft in commercial for-hire or leased vehicles.
  - Shipments (except laboratory analysis samples or reference materials) must be made by a mode of transportation that can be traced and that provides for determination, within 24 hours of request, of the last known location of the shipment. This process must be implemented if a shipment fails to arrive at its destination at the prescribed time.
  - Shippers are required to give the consignee an estimated time of arrival before dispatch and to follow up with a written confirmation not later than 48 hours after dispatch.
  - Consignees must promptly notify the shipper by telephone and written confirmation upon determination that a shipment has not arrived by the scheduled time. Upon initial notification, the shipper must report the situation commensurate with procedures given in DOE M 470.4-1, Safeguards and Security Program Planning and Management.

**f) Describe escort responsibilities when special nuclear material is in transit.**

*CAT I and II Quantities of SNM*

Escort responsibilities for transit of CAT I and II quantities of SNM include the following:

- Domestic off-site SNM shipments must be made by OST.
- Protection measures for movements of the SNM, between PAs at the same site or between PAs and staging areas on the same site, must be under constant surveillance by armed PF escorts.

*CAT III Quantities of SNM*

Escort responsibilities for transit of CAT III quantities of SNM include the following:

- Truck or Train Shipment. Shipment escorts must periodically communicate with a control station operator. The control station operator must be capable of requesting appropriate local law enforcement agency response if needed.
- Air Shipment. Shipments must be under the direct observation of the authorized escorts during all land movements and loading and unloading operations.

**g) Discuss the protection provided to vital equipment.**

SSPs and SSSPs must define applicable threats to and protection measures for vital equipment.

**5. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of security areas as described in DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests.**

Note: DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-2, Physical Protection, and DOE M 470.4-4, Information Security.

**a) Describe the different security areas.**

Security areas include PPAs, LAs, EAs, PAs, vital areas, MAAs, and specially designated security areas (e.g., Sensitive Compartmented Information Facilities [SCIFs] and Special Access Program Facilities [SAPFs]).

*Property Protection Areas*

PPAs are established to protect Government-owned property against damage, destruction, or theft. Protection may include physical barriers, access control systems, protective personnel or persons assigned administrative or other authorized security duties, IDSs, and locks and keys. The designation and description of PPA protective measures must be approved by DOE line management (e.g., SSP or SSSP). The requirements for PPAs must be configured to protect Government-owned property and equipment against damage, destruction, or theft, and must provide a means to control public access.

*Limited Areas*

LAs are security areas designated for the protection of classified matter and Category III quantities of SNM. LAs are defined by physical barriers encompassing the designated space and access controls to ensure that only authorized personnel are allowed to enter and exit the area. A means must be provided to detect unauthorized entry into the LA.

*Exclusion Areas*

EAs are security areas in which an individual's mere presence may result in access to classified matter. The boundaries of EAs must be encompassed by physical barriers. EAs require access controls that ensure only authorized personnel are allowed to enter and exit the area. Examples of means to detect unauthorized entry into the EA include PF patrols, closed circuit television systems, IDSs, or a combination of measures. Unauthorized entry into the EA must be detected.

*Protected Areas*

PAs are security areas used to protect Category II or greater quantities of SNM and to provide security zones surrounding separately defined MAAs. PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a PIDAS, and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.

*Vital Areas*

Vital areas are separate security areas that contain vital equipment within PAs. In addition to the protection strategies required for PAs, the following requirements must be applied:

- Boundaries must conform to the layered protection concept, with a separate vital area perimeter located within a PA.
- The perimeter must be monitored to deter and detect unauthorized entry attempts.
- Vital equipment must be protected with an IDS.
- Exits must be alarmed or controlled at all times.
- PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.
- All requirements for personnel and vehicle access control that apply to PAs apply to vital areas.

*Material Access Areas*

MAAs are security areas used to protect Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity. MAAs must have defined boundaries with barriers that provide sufficient delay time to impede, control, or deter unauthorized access.

*Special Designated Security Areas*

Other areas with access restrictions include CASs, SASs, SCIFs, SAP facilities, local law enforcement agencies, private alarm stations, secure communications centers, and automated information system centers.

**b) Discuss controls to detect, assess, deter, and prevent unauthorized access to Security Areas.**

Personnel, hand-carried items, deliveries/mail, vehicles, and vehicle contents are subject to random inspections at security area boundaries except for PAs and MAAs, where inspections are mandatory. The cognizant security authority must approve local procedures that implement requirements for access control and entry/exit inspections. The requirements addressed below apply to all security areas except PPAs.

*Access Control*

Access must be based on an individual's "need to know" to perform official duties, validation of the individual's access authorization, and the presentation of a DOE security badge. A person allowed to enter an LA, EA, PA, vital area, or MAA without an appropriate access authorization must be escorted at all times by an individual with

- knowledge of security procedures for the security areas to prevent compromise of classified information or matter
- appropriate access authorization
- "need to know" for the security area or the S&S interests

*Badge Validation*

Access to a security area requires verification of an access authorization and a valid DOE security badge.

*Layered Access Controls*

Access control requirements must be layered in a graded manner at successive boundaries, as appropriate for the situation.

*Piggybacking*

Authorized personnel are permitted to vouch for an individual, providing all access authorization and "need to know" requirements are met.

*Entry Control Point Functions*

The following must be performed at entry control points:

- Prohibit entry until access is authorized.
- Permit entry of only one person at a time into PAs and MAAs.
- Control access when going from one security area into another security area with increased protection requirements.
- Perform entry and exit inspections to deter introduction of unauthorized personnel, prohibited and controlled articles, and unauthorized removal of S&S interests.

*Entry/Exit Inspections*

The following requirements apply to entry and exit inspections. The inspection process must be documented in the SSSP or SSP.

- An inspection program must ensure prohibited and controlled articles are detected before being brought into facilities. Likewise, such programs must ensure S&S interests are not removed.
- Passage of individuals, vehicles, and/or packages or mail through entry control point inspection equipment must be observed and controlled by protective personnel. Handheld and/or portable detectors, etc., must be available to resolve alarms and for use during inspection equipment failures. Inspection equipment can include metal detectors, SNM detectors, explosive detectors, and x-ray systems, and must ensure that prohibited and controlled articles are detected before being brought into DOE facilities.
- Bypass routes around inspection equipment must be closed or monitored to deter unauthorized passage of personnel and hand-carried articles.
- Auxiliary power must be provided to all control point inspection equipment.
- Measures must be taken to preclude the unauthorized alteration of control settings on all entry/exit control point inspection equipment.
- Equipment must have both audible and visual alarms monitored by on-post PF personnel.
- Ingress/egress points must be designed to preclude commingling of searched and unsearched personnel.

*Entry Inspection Procedures*

All personnel, vehicles, packages, and hand-carried articles are subject to inspection before entry into a security area.

*Exit Inspection Procedures*

Personnel, vehicles, and hand-carried items, including packages, briefcases, purses, and lunch containers, are subject to exit inspections to deter and detect unauthorized removal of classified matter or other S&S interests from security areas. Collocated SNM detectors and metal detectors must be used at PAs and/or MAAs to inspect personnel for SNM.

*Automated Access Control Systems*

Automated access control systems may be used if the following requirements are met:

- Automated access controls used for access to any security area must verify that the access authorization and the DOE security badge are valid (i.e., that the badge serial number read by the system matches the serial number assigned to the badge holder). Badges must be validated by means of a PIN or other approved means.
- When remote, unattended, automated access control system entry control points are used for access to security areas, the barrier must be resistant to bypass.
- Automated access control system intrusion alarms (e.g., annunciation of a door alarm, duress alarm, tamper alarm, or anti-passback indication feature) must be treated in the same manner as an intrusion alarm for the area being protected.

**c) Describe when random entry/exit inspections are permitted and give reasons for those inspections.**

Personnel, hand-carried items, deliveries/mail, vehicles, and vehicle contents are subject to random inspections at security area boundaries except for PAs and MAAs, where inspections are mandatory. The cognizant security authority must approve local procedures that implement requirements for access control and entry/exit inspections.

**d) Describe the articles prohibited from Security Areas cited in 10 CFR part 860, Trespassing on Administration Property, and Title 41 CFR Part 101, Federal Property Management Regulations.**

The articles listed below are not permitted in any security area without authorization, unless identified in approved local procedures:

- Explosives
- Dangerous weapons
- Instruments or material likely to produce substantial injury to persons or damage to persons or property
- Controlled substances (e.g., illegal drugs and associated paraphernalia, but not prescription medicine)
- Any other items prohibited by law

Specific information covering prohibited items may be found under the provisions of 10 CFR 860 and 41 CFR 101-20.3.

**e) List the types of privately owned articles prohibited from a security area.**

Portable electronic devices capable of recording information or transmitting data (e.g., radio frequency, infrared, and/or data link electronic equipment) are not permitted in LAs, EAs, PAs, vital areas, MAAs, SCIFS, or SAPFs without authorization.

**f) Describe the level of protection given to a property protection area.**

Protection may include physical barriers, access control systems, protective personnel or persons assigned administrative or other authorized security duties, IDSs, and locks and keys. The designation and description of PPA protective measures must be approved by DOE line management (e.g., SSP or SSSP). The requirements for PPAs must be configured to protect

Government-owned property and equipment against damage, destruction, or theft, and must provide a means to control public access.

**g) Describe the level of protection, access requirements, and storage requirements for a limited area.**

LAs are security areas designated for the protection of classified matter and Category III quantities of SNM. LAs are defined by physical barriers encompassing the designated space and access controls to ensure that only authorized personnel are allowed to enter and exit the area. A means must be provided to detect unauthorized entry into the LA.

LA access requirements must be administered as explained below.

Individuals without appropriate access authorization must be escorted by an authorized individual who must ensure measures are taken to prevent compromise of classified matter or access to SNM. Access to S&S interests not in approved storage within an LA must be controlled by the custodian or authorized user. The identity and access authorization of each person seeking entry must be validated by appropriately authorized personnel, automated systems, or other means documented in the SSSP or SSP. Where practicable, PF personnel will not be used to control access to LAs.

Private vehicles are prohibited from LAs unless specifically authorized in writing. Approval authority for non-Government vehicle access must be documented in the SSSP or SSP.

Government-owned or Government-leased vehicles may be admitted only when on official business and only when operated by properly cleared and authorized drivers or when the drivers are escorted by properly cleared and authorized personnel. The SSSP or SSP must identify procedures for inspection of and access by service and delivery vehicles.

When a remote automated access control system is used for vehicle access control, it must verify that the operator or the escort has a valid DOE security badge (i.e., the badge serial number read by the system must match the serial number assigned to the badge holder) and a valid access authorization.

**h) Describe the level of protection, access requirements, and storage requirements for an exclusion area.**

The boundaries of EAs must be encompassed by physical barriers. EAs require access controls that ensure only authorized personnel are allowed to enter and exit the area. Examples of means to detect unauthorized entry into the EA include PF patrols, closed circuit television systems, IDSs, or a combination of measures. Unauthorized entry into the EA must be detected.

EA access requirements are as follows:

- Individuals who are permitted unescorted access must have "L" or "Q" access authorizations and a "need to know" consistent with the classified matter to which they have access by virtue of their presence in the area.
- Individuals without "L" or "Q" access authorization and "need to know" must be escorted by a knowledgeable individual who must ensure measures are taken to prevent compromise of classified matter.

*Personnel and Vehicle Access Control*

Site/facility-authorized personnel and/or automated systems at entrances must validate the identity and access authorization of persons allowed access. All requirements for personnel and vehicle access control that apply to LAs apply to EAs.

Classified matter in EAs must be processed, handled, or stored so that protection measures are equal to or greater than those present in an LA.

**i) Describe the level of protection for a protected area.**

PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a PIDAS, and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.

- Vehicle barriers must be installed to delay penetrations of the security area.
- PA barriers must be designed to delay and/or deter unauthorized access.
- The barrier design must allow entry control points for appropriate personnel, vehicles, and materials/packages while deterring or preventing an insider from diverting material past the barrier for retrieval.
- The barrier design must consider proximity to buildings or overhanging structures.
- The barrier design must consider the attempted removal of S&S interests by an insider.

**j) Discuss function and performance of personnel entry/exit and vehicle entry inspections for those entering a protected area.**

Entrance inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect prohibited and controlled articles. Exit inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect the unauthorized removal of SNM and other Government property. Specific inspection procedures with limitations and thresholds for SNM detectors and metal detectors must be established and documented in the SSSP or SSP.

Exit inspection procedures must be written to ensure

- the identification of detection thresholds for SNM and shielding that are consistent with the SNM type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of SNM contained within the area;
- the detection of shielded SNM (e.g., by using a combination of SNM detectors and metal detectors);
- that entry control points without the means to detect SNM are not used to exit, except in emergencies;
- the conduct of random exit inspections at a PA boundary, when a PA encompasses an MAA and the Category II or greater quantities of SNM are contained completely within the MAA (the frequency must be determined by DOE line management);
- that equivalent protection measures are implemented when emergency exits are used (e.g., searches are conducted at an assembly area).

**k) Describe the response to an intrusion alarm within a protected area.**

PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.

**l) Describe the level of protection and access requirements for a Vital Area.**

In addition to the protection strategies required for PAs, the following requirements must be applied to vital areas:

- Boundaries must conform to the layered protection concept, with a separate vital area perimeter located within a PA.
- The perimeter must be monitored to deter and detect unauthorized entry attempts.
- Vital equipment must be protected with an IDS.
- Exits must be alarmed or controlled at all times.
- PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.
- All requirements for personnel and vehicle access control that apply to PAs apply to vital areas.

**m) Describe the level of protection for a material access area.**

MAAs must have defined boundaries with barriers that provide sufficient delay time to impede, control, or deter unauthorized access. Additionally, the following requirements apply:

- MAAs must be located within a PA, but must be separate and distinct (i.e., no shared boundaries); however, multiple MAAs may exist within a single PA. An MAA cannot cross a PA boundary.
- Barriers must delay or deter the unauthorized movement of SNM while allowing access by authorized personnel and material movement through entry control points and emergency evacuation as necessary. Doors at entry control points such as transfer locations must be alarmed, and the alarms must communicate with the CAS/SAS when an unauthorized exit occurs.
- PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.
- Penetrations in the floors, walls, or ceilings for piping, heating, venting, air conditioning, or other support systems must not create accessible paths that could facilitate the removal or diversion of S&S interests.
- Exits designed for emergency evacuation must be alarmed with an IDS or controlled at all times.
- Active and passive denial systems will be deployed, as appropriate, to reduce reliance on recapture operations.

**n) Discuss the entry/exit inspections required for a material access area.**

The following are entry/exit inspection requirements for MAAs:

- Entrance inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect prohibited and controlled articles.

- Exit inspections of all personnel, vehicles, packages, and hand-carried items must be performed to deter and detect the unauthorized removal of SNM and other Government property. Specific inspection procedures with limitations and thresholds for SNM detectors and metal detectors must be established and documented in the SSSP or SSP.
- A separate physical or electronic inspection of each vehicle, person, package, and container must be conducted at all MAA exit points.
- Exit inspection procedures and detection thresholds for SNM and shielding must be established consistent with the SNM type, form, quantity, attractiveness level, size, configuration, portability, and credible diversion amounts of SNM contained within the MAA.
- Exit inspections must be capable of detecting shielded SNM (e.g., by using a combination of SNM detectors and metal detectors).

**o) Describe the response to an intrusion alarm within a material access area.**

Top Secret must be stored in a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.

Secret must be stored in a locked VTR within an LA, EA, PA, or MAA equipped with IDS protection. The PF must respond within 30 minutes of alarm annunciation.

**p) Describe the level of protection for Sensitive Compartmented Information Facilities.**

DOE follows the requirements in Director of Central Intelligence Directive 6/9, DOE Order 5639.8A, Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities, dated July 23, 1993, and the DOE Sensitive Compartmented Information Facility Procedural Guide for the construction and accreditation of SCIFs.

**6. Safeguards and security personnel acting in physical security shall demonstrate a working-level knowledge of security areas as described in DOE Order 473.2, Protective Force Programs.**

Note: DOE O 473.2, Protective Force Programs, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-3, Protective Force, 10 CFR 1047, Limited Arrest Authority and Use of Force by Protective Force Officers, and 10 CFR 1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve.

**a) Describe the requirements for an armed protective force.**

Within DOE, armed PFs exist to deter and to defeat terrorist or other adversarial actions that could have major national security consequences, primarily, unauthorized access to nuclear weapons and components, special nuclear material, or targets subject to chemical, biological, or radiological sabotage or that contain a unique capability that must be protected. When availability of armed PFs is limited, they shall not be used to: perform routine, repetitive tasks that are not related directly to target protection; perform access control functions that can be better accomplished through automation; act as administrative escorts for construction projects or

service personnel (unless required for protection of assets); or staff posts that offer convenience to management and/or employees.

**b) Discuss how responsibilities identified in a protective force job analysis relate to proficiency in the skills and abilities necessary to perform job tasks.**

DOE personnel responsible for training FO/FA/SA personnel must prepare and annually (at least every 12 months) review a job analysis (JA) detailing the required actions or functions for each specific job assignment. The JA must be used as a basic input document for local training requirements, and must be approved by the DOE cognizant security authority and reviewed and updated annually (at least every 12 months).

The qualification requirements will be supported by a formal training program that develops and maintains the knowledge, skills, and abilities required to perform assigned tasks.

**c) Discuss specific laws regarding property of the United States and provisions of the Atomic Energy Act, as described in 10 CFR 1047, Defense Programs; Limited Arrest Authority and Use of Force by Protective Force Officers, and 1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve.**

Under the Atomic Energy Act, the authority of a DOE PF officer to arrest without warrant is limited to the performance of official duties and should be exercised only in the enforcement of the following laws, and only if property of the United States which is in the custody of the DOE or its contractors is involved.

Felonies.

- Arson — 18 U.S.C. 81 (only applicable to ‘‘special maritime and territorial jurisdiction of the United States’’ as defined by 18 U.S.C.7)
- Building or property within special maritime and territorial jurisdiction — 18 U.S.C. 1363 (only applicable to ‘‘special maritime and territorial jurisdiction of the United States’’ as defined by 18 U.S.C. 7)
- Civil disorder — 18 U.S.C. 231
- Communication lines, stations, or systems — 18 U.S.C. 1362
- Concealment, removal, or mutilation generally — 18 U.S.C. 2071
- Conspiracy — 18 U.S.C. 371 (violation of this section is a felony if the offense which is the object of the conspiracy is a felony)
- Destruction of motor vehicles or motor vehicle facilities — 18 U.S.C. 33
- Explosives — 18 U.S.C. 844(f)
- Government property or contracts — 18 U.S.C. 1361 (violation of this section is a felony if property damage exceeds $100)
- Military, naval, or official passes — 18 U.S.C. 499 (pertains to forging or altering official passes)
- Personal property of the United States — 18 U.S.C. 2112
- Public money, property, or records — 18 U.S.C. 641 (violation of this section is a felony if the property value exceeds $100)
- Sabotage — 18 U.S.C. 2151, 2153–2156
- Violation under Physical Security Convention — 18 U.S.C. 831

Misdemeanors.

- Conspiracy — 18 U.S.C. 371 (violation of this section is a misdemeanor if the offense which is the object of the conspiracy is a misdemeanor)
- Explosives — 18 U.S.C. 844(g)
- Government property or contracts — 18 U.S.C. 1361 (violation of this section is a misdemeanor if the property damage does not exceed $100)
- Official badges, identification cards, other insignia — 18 U.S.C. 701 (pertains to the manufacture, sale, and possession of official insignia)
- Public money, property, or records — 18 U.S.C. 641 (violation of this section is a misdemeanor if the property value does not exceed $100)

**d) Discuss the Departmental policy on the use of deadly force and limited arrest authority as set forth in 10 CFR 1047, Defense Programs; Limited Arrest Authority and Use of Force by Protective Force Officers, and 1049, Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve.**

*Arrest Authority*

Felony Arrests. A PF officer is authorized to make an arrest for any felony listed in 10 CFR 1047 if the offense is committed in the presence of the PF officer or if he or she has reasonable grounds to believe that the individual to be arrested has committed or is committing the felony. In the presence of means that the criminal act must have taken place in the physical presence of (under the observation of) the PF officer. Knowledge of the existence of a criminal violation obtained in any other way (e.g., information from other persons) is not sufficient to permit an arrest. Reasonable grounds to believe means that, at the moment of arrest, either the facts and circumstances within the knowledge of the PF officer, or of which the PF officer had reasonably trustworthy information, were sufficient to cause a prudent person to believe that the suspect had committed or was committing the offense.

Misdemeanor Arrest. A PF officer is authorized to make an arrest for any misdemeanor listed in 10 CFR 1047 if the offense is committed in the presence of the PF officer.

*Other Authority*

The Atomic Energy Act does not provide authority to arrest for violations of state criminal statutes or for violations of federal criminal statutes other than those listed in 10 CFR 1047. Therefore, arrests for violations of such other criminal statutes shall be made by other peace officers (e.g., U.S. Marshals or FBI agents for federal offenses; local law enforcement agency officers for state or local offenses) unless the PF officer can make a citizen's arrest for the criminal offense under the law of the state, the PF officer is an authorized state peace officer or otherwise deputized by the particular state to make arrests for state criminal offenses, or the PF officer has been deputized by the U.S. Marshals Service or other federal law enforcement agency to make arrests for the criminal offense. In those locations which are within the ''special maritime and territorial jurisdiction of the United States,'' as defined in 18 U.S.C. 7, the Assimilative Crimes Act (18 U.S.C. 13) adopts the law of the state for any crime under state law not specifically prohibited by federal statute and provides for federal enforcement of that state law. The local DOE Office of Chief Counsel, in coordination with contractor legal counsel, as appropriate, shall provide guidance in this matter.

*Arrest authority for the Strategic Petroleum Reserve (SPR)*

Under the Atomic Energy Act, the authority of a DOE PF officer to arrest without warrant is to be exercised only in the performance of the official duties of protecting the SPR and persons within or upon the SPR.

A PF officer is authorized to make an arrest for a felony committed in violation of laws of the United States, or for a misdemeanor committed in violation of laws of the United States if the offense is committed in the officer's presence.

A PF officer also is authorized to make an arrest for a felony committed in violation of laws of the United States if the officer has reasonable grounds to believe that the felony has been committed, or that the suspect is committing the felony, and is in the immediate area of the felony or is fleeing the immediate area of the felony.

*Use of Deadly Force*

Deadly force is that force which a reasonable person would consider likely to cause death or serious bodily harm. Its use may be justified only under conditions of extreme necessity, when all lesser means have failed or cannot reasonably be employed. A PF officer is authorized to use deadly force only when one or more of the following circumstances exist:

- Self-Defense — when deadly force reasonably appears to be necessary to protect a PF officer who reasonably believes himself or herself to be in imminent danger of death or serious bodily harm.
- Serious Offenses Against Persons — when deadly force reasonably appears to be necessary to prevent the commission of a serious offense against a person(s) in circumstances presenting an imminent danger of death or serious bodily harm (e.g. sabotage of an occupied facility by explosives).
- Nuclear Weapons or Nuclear Explosive Devices — when deadly force reasonably appears to be necessary to prevent the theft, sabotage, or unauthorized control of a nuclear weapon or nuclear explosive device.
- Special Nuclear Material — when deadly force reasonably appears to be necessary to prevent the theft, sabotage, or unauthorized control of SNM from an area of a fixed site or from a shipment where Category II or greater quantities are known or reasonably believed to be present.
- Apprehension — when deadly force reasonably appears to be necessary to apprehend or prevent the escape of a person reasonably believed to have committed an offense considered by the Department of Energy to pose a significant threat of death or serious bodily harm, or to be escaping by use of a weapon or explosive, or who otherwise indicates that he or she poses a significant threat of death or serious bodily harm to the PF officer or others unless apprehended without delay.

*Additional Considerations Involving Firearms*

If it becomes necessary to use a firearm, the following precautions shall be observed:

- A warning, e.g., an order to halt, shall be given, if feasible, before a shot is fired.
- Warning shots shall not be fired.

**e) Discuss firearms safety procedures related to issue duty weapons.**

The four general firearms safety rules are as follows:

- All firearms are always loaded.
- Never point a firearm at anything you are not willing to destroy.
- Keep your finger off the trigger until your sights are on the target.
- Be sure of your target.

Specific range safety rules are listed below:

- It is mandatory to use approved eye and ear protection and other personal protective equipment as required by the range safety officer.
- Unsafe conditions must be reported immediately to an instructor.
- A firearm may only be exchanged with another shooter under the direct supervision of an instructor.
- Firearms must not be left unattended or unsecured.
- Firearm loading and firing may commence only on command.
- Shooters are not permitted to talk during a firing activity except in reply to an instructor as a part of the activity or to shout "cease fire" in an unsafe situation.
- Until the firing line has been declared safe by the firearms instructor, shooters must not move past or bend over the line.
- All shooters must be trained on what constitutes an unsafe condition and to shout "cease fire" when such a condition is observed.
- Smoking, eating, or drinking must be prohibited while shooting.
- Alcoholic beverages and drugs are prohibited on firing ranges. Shooters taking medication must report this fact to the firearms instructor before reporting to the firing line. The firearms instructor is responsible for determining whether a shooter is fit based on the medication taken and whether it is safe for the shooter to use the range. A physician may be consulted if necessary.
- Shooters must take precautions to prevent hot spent cartridge and gunshot residues from getting inside their clothing.
- When a training session is completed, each firearm must be physically examined by the shooter and by a designated range safety officer or qualified firearms instructor to ensure that it is unloaded and in safe condition before leaving the range. If the shooter is using a duty firearm on the range, he or she may reload that weapon at the range if returning directly to duty.
- Shooters must collect unexpended ammunition and return it to a firearms instructor.
- While a firearm is being cleaned, live ammunition must not be allowed in the cleaning area.

**f) Discuss firearms qualification requirements for all issued duty weapons.**

*Training of PF Officers and Qualification to Carry Firearms*

PF officers shall successfully complete training required by applicable DOE Orders prior to receiving authorization to carry firearms. The DOE Office of Safeguards and Security shall approve the course.

Prior to initial assignment to duty, PF officers shall successfully complete a basic qualification training course which equips them with at least the minimum level of

competence to perform tasks associated with their responsibilities. The basic course shall include the following subject areas:

- Legal authority, including use of deadly force and exercise of limited arrest authority
- Security operations, including policies and procedures
- Security tactics, including tactics for PF officers acting alone or as a group
- Use of firearms, including firearms safety and proficiency with all types of weapons expected to be used
- Use of non-deadly weapons, weapon-less self-defense, and physical conditioning
- Use of vehicles, including vehicle safety in routine and emergency situations
- Safety, first aid, and elementary firefighting procedures
- Operating in such a manner as to preserve SPR sites and facilities
- Communications, including methods and procedures

After completing training, and receiving the appropriate security clearance, PF officers shall be authorized to carry firearms and exercise limited arrest authority. PF officers shall receive an identification card, which must be carried whenever on duty and whenever armed.

On an annual basis, each PF officer must successfully complete training sufficient to maintain at least the minimum level of competency required for the successful performance of all assigned tasks identified for PF officers.

PF officers shall be qualified in the use of firearms by demonstrating proficiency in the use of firearms on a semiannual basis prior to receiving authorization to carry firearms. PF officers shall demonstrate proficiency in the use of all types of weapons expected to be used while on duty under both day and night conditions. In demonstrating firearms proficiency, PF officers shall use firearms of the same type and barrel length as firearms used by PF officers while on duty, and the same type of ammunition as that used by PF officers on duty. Before a PF officer is qualified in the use of firearms, the officer shall complete a review of the basic principles of firearms safety.

PF officers shall be allowed two attempts to qualify in the use of firearms. PF officers shall qualify in the use of firearms within six months of failing to qualify. If an officer fails to qualify, the officer shall complete a remedial firearms training program. A PF officer who fails to qualify in the use of firearms after completion of a remedial program and after two further attempts to qualify shall not be authorized to carry firearms or to exercise limited arrest authority.

**g) Discuss application of the authorization to carry firearms and make arrests without a warrant while performing official duties.**

*Exercise of Arrest Authority — General Guidelines*

In making an arrest, and before taking a person into custody, the PF officer should

- announce the PF officer's authority (e.g., by identifying himself as an SPR PF officer)
- state that the suspect is under arrest
- inform the suspect of the crime for which the suspect is being arrested

If the circumstances are such that making these announcements would be useless or dangerous to the officer or to another person, the PF officer may dispense with these announcements.

At the time and place of arrest, the PF officer may search the person arrested for weapons and criminal evidence, and may search the area into which the person arrested might reach to obtain a weapon or to destroy evidence.

After the arrest is effected, the person arrested shall be advised of his constitutional right against self-incrimination (''*Miranda* warnings''). If the circumstances are such that immediately advising the person arrested of this right would result in imminent danger to the officer or other persons, the PF officer may postpone this requirement. The person arrested shall be advised of this right as soon as practicable after the imminent danger has passed.

As soon as practicable after the arrest is effected, custody of the person arrested should be transferred to other federal law enforcement personnel (e.g., U.S. Marshals or FBI agents) or to local law enforcement personnel, as appropriate, in order to ensure that the person is brought before a magistrate without unnecessary delay.

Ordinarily, the person arrested shall not be questioned or required to sign written statements unless such questioning is

- necessary to establish the identity of the person arrested and the purpose for which such person is within or upon the SPR
- necessary to avert an immediate threat to security or safety (e.g., to locate a bomb)
- authorized by other federal law enforcement personnel or local law enforcement personnel responsible for investigating the alleged crime

**h) Describe the situations in which fresh pursuit guidelines and site-specific guidelines for fresh pursuit of criminals are invoked.**

Fresh pursuit is defined as pursuit (with or without a warrant) for the purpose of preventing the escape or effecting the arrest of any person who commits a misdemeanor or felony or is suspected of having committed a misdemeanor or felony. Fresh pursuit implies pursuit without unreasonable delay, but which need not be immediate pursuit. (Although fresh pursuit implies pursuit without unreasonable delay, for the purpose of preventing the escape or effecting the arrest of fleeing, suspected criminals who are in unauthorized control or possession of nuclear weapons, weapons components, and/or SNM, such pursuit must be effected immediately.)

It is DOE policy to prevent the escape and effect the arrest of fleeing suspected criminals in a safe and expeditious manner. Each site must prepare site-specific guidelines that take into account the geography, equipment, and functions of the facility/site, and that address the procedures that will be used to provide emergency notification to jurisdictions that may be entered in a fresh pursuit situation. The DOE cognizant security authority must submit the guidelines through the cognizant Departmental element to the Director, Office of Security, for approval.

The following apply to authorized pursuit across jurisdictional lines:

- Misdemeanors. A PF officer may engage in the fresh pursuit of a suspected misdemeanant across jurisdictional lines only if the alleged misdemeanor was committed, or is being committed, in his or her presence.
- Felonies. PF officers may engage in the fresh pursuit of a suspected felon across jurisdictional lines if the alleged felony is being committed, or was committed, in the presence of a PF officer, and any PF officer has reasonable grounds to believe that the person pursued is committing, or has committed, the alleged felony.

In making fresh pursuit decisions, PF officers must consider applicable federal and state laws; Departmental directives, guidelines, and regulations; and PF plans, post orders, general orders, guidelines, and training.

**i) Describe safety procedures in fresh pursuit.**

Safety is a primary consideration when engaged in fresh pursuit of a suspected criminal. In determining whether to pursue, as well as the method and means of pursuit, a PF officer will weigh the seriousness of the alleged offense and the necessity for immediate apprehension against the risk of injury to himself/herself, other PF officers, and the public. If at any time during the pursuit the risk of injury to pursuing PF officers or the public surpasses the necessity for immediate apprehension, the pursuit must be terminated. PF officers will use the minimum force necessary under the circumstances to apprehend a suspected criminal.

Regulations in 10 CFR 1047.6, 1047.7, 1049.6, and 1049.7 address the applicability of physical and/or deadly force in a fresh pursuit situation, regardless of whether jurisdictional lines have been crossed. Such use may include, as appropriate, firing at or from a moving vehicle, aircraft, or water craft; the ramming and disabling of pursued vehicles by precision immobilization techniques; and the use of tire deflating devices.

If hostages are present in a pursuit situation in which recovery of SNM is involved, the safety and welfare of hostages must be considered; however, due to the ramifications of unauthorized use of SNM to the national security, the public, and the environment, the hostages' presence must not deter or impact immediate pursuit and recovery of the SNM.

**j) Describe the difference between a misdemeanor and a felony.**

A felony is any offense enumerated in 10 CFR, 1047.4(a)(1)(i), as well as any offense constituting a felony under the laws of the jurisdiction in which the facility is located and with respect to which a PF officer would have arrest authority under 10 CFR 1047.4(d) and (e).

A misdemeanor is any offense enumerated in 10 CFR 1047.4(a)(1)(ii), as well as any offense constituting a misdemeanor under the laws of the jurisdiction in which the facility is located and with respect to which a PF officer would have arrest authority under 10 CFR 1047.4(d) and (e).

A felony, in many common law legal systems, is the term for a "very serious" crime, whereas misdemeanors are considered to be less serious offenses. Crimes which are commonly considered to be felonies include, but are not limited to, aggravated assault, arson, burglary, murder, and rape. Those who are convicted of a felony are known as felons. Felons can receive punishments which range in severity from probation, to imprisonment, to execution.

In the United States, felons often receive additional punishments such as the loss of voting rights, exclusion from certain lines of work, prohibition from obtaining certain licenses, exclusion from purchase/possession of firearms or ammunition, and ineligibility to run for or be elected to public office.

**7. Safeguards and security personnel acting in physical security shall demonstrate the ability to review the contractor's protection program for approval as described in DOE O 470.1, Chapter III, Performance Assurance Program.**

**a) Conduct an assessment of the contents and accuracy of the contractor's protection and control planning.**

**b) Assess the contractor's methods for protecting special nuclear material and vital equipment.**

**c) Assess the contractor's program for protecting and controlling classified matter.**

**d) Review and approve the contractor's program for protecting and controlling unclassified irradiated reactor fuel in transit.**

**e) Assess the contractor's program for establishing, controlling, and maintaining security and restricted access areas.**

**f) Assess and approve the following protection elements established by the contractor:**
- **Intrusion detection and assessment systems**
- **Control and entry/exit inspections**
- **Barriers and locks**
- **Secure storage**
- **Communications**
- **Acceptance and validation testing**
- **Maintenance**
- **Posting notices**
- **Security badges and credentials**

**g) Review for approval the contractor's protective force orders, plans, and procedures.**

Elements "a" through "g" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**8. Safeguards and security personnel acting in physical security shall demonstrate the ability to assess the contractor's protection program operations in accordance with DOE O 473.2, Protective Force Programs.**

**a) Assist in designing and evaluating a force-on-force performance test.**

**b) Assist in designing and evaluating an emergency management performance test.**

**c) Assist in designing and evaluating a limited scope performance test of protective forces.**

Elements "a" through "c" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**9. Safeguards and security personnel acting in personnel security shall demonstrate a working-level knowledge of the access authorization (security clearance) process.**

**a) Discuss the following terms:**
- **Derogatory information**
- **Access authorization**
- **Single scope background investigation**
- **Suspension**

*Derogatory Information*

Derogatory information includes
- any factual and verifiable unfavorable information that creates a question as to an individual's eligibility for an access authorization or an entity's eligibility for a favorable foreign ownership, control, or influence determination;
- any information that adversely reflects on the integrity or character of a cleared employee that suggests his or her ability to protect classified information may be impaired, or that his or her access to classified information clearly may not be in the interest of national security (National Industrial Security Program Operating Manual);
- any information that adversely reflects on the ethics and compliance program of a company with a cleared facility that suggests the company's ability to protect classified information and/or special nuclear material may be impaired.

*Access Authorization*

Access authorization is an administrative determination that an individual is eligible for access to classified matter when required by official duties or is eligible for access to, or control over, special nuclear material.

*Single-Scope Background Investigation (SSBI)*

An SSBI is a background investigation consisting of record reviews and indices checks, a subject interview, and interviews with sources of information as specified in the "Investigative Standards for Background Investigations for Access to Classified Information," which implement Executive Order 12968. This type of investigation is used as a basis for initially determining an individual's eligibility for a Q access authorization, a Top Secret security clearance, or access to sensitive compartmented information.

*Suspension*

A suspension is a cancellation of access authorization.

**b) Discuss the process for screening reports of investigation for initial Q and L access authorizations.**

The investigative standard for a Q access authorization is a Single Scope Background Investigation (SSBI). The investigation for an L access authorization processed before October 1997 was a National Agency Check with Credit (NACC). For L access authorization requests initially processed after October 1997, the investigation is a National Agency Check with Law and Credit (NACLC) for non-federal employees and an Access National Agency Check and Inquiries (ANACI) for federal employees.

**c) Explain the relevance in terms of risk assessment of the clearance criteria in 10 CFR 710, Subpart A, General Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material.**

Favorable and unfavorable investigative information must be analyzed according to the criteria found in 10 CFR 710.8. Frequently, the reported derogatory information alone raises a security concern, but may be resolved when considered with other reported mitigating information.

**d) Explain the purpose of the personnel security interview.**

When information contained in investigative reports or the receipt of other reliable information raises a question concerning an individual's eligibility for an access authorization, additional actions, such as a personnel security interview (PSI), may be authorized for collecting relevant information pertaining to the eligibility determination. PSIs must be conducted only by personnel security specialists appropriately trained and cognizant of all the questions or items of information to be explored. DOE F 5631.5, The Conduct of Personnel Security Interviews under DOE Security Regulation, and DOE F 5631.7, Privacy Act Statement for Personnel Security Interviews and Release Forms Related Thereto, must be properly executed for all PSIs. All PSIs will be audio or audio/video recorded. The PSI will then be transcribed or summarized. If a transcript is not prepared, the recorded PSI must be retained and protected in the same manner as the PSF.

**10. Safeguards and security personnel acting in personnel security shall demonstrate a familiarity-level knowledge of security awareness activities.**

**a) Discuss the purposes for conducting the following types of briefings:**
- **Initial**
- **Comprehensive**
- **Refresher**
- **Termination**

*Initial Briefing*

Personnel who receive a DOE security badge must receive an initial briefing before they are given unescorted access.

*Comprehensive Briefing*

An individual must receive a comprehensive briefing upon receipt of an access authorization and before receiving initial access to classified information or matter, or SNM.

The content for the comprehensive briefing must include the following classification and declassification requirements and procedures items:
- Definition of classified information or matter
- Purpose of the DOE classification and declassification program
- Levels and categories of classified information or matter
- Damage criteria associated with each classification level
- Authority for classification and declassification
- Procedures for challenging the classification status of information

*Refresher Briefing*

Cleared individuals must receive annual (at least every 12 months) refresher briefings. Agreements between DOE elements and/or contractor organizations may be established to ensure that individuals temporarily assigned to other DOE locations receive refresher briefings on schedule. Refresher briefings must selectively reinforce the information provided in the comprehensive briefing. Refresher briefings must also address current facility-/organization-specific S&S issues and counterintelligence (CI) awareness.

*Termination Briefing*

A termination briefing is required whenever an access authorization has been or will be terminated. Termination briefings must reiterate to the individual the continuing responsibility not to disclose classified information or matter to which they had access, the potential penalties for noncompliance, and the obligation to return all unclassified controlled and classified documents and materials in the individual's possession to the cognizant security authority or to the DOE.

The content for the termination briefing must include

- information contained in items 1 through 6 of the Security Termination Statement Form (DOE F 5631.29);
- information contained in items 3, 4, 5, 7, and 8 of the SF 312;
- penalties for unauthorized disclosure of classified information or matter as specified in the Atomic Energy Act of 1954;
- penalties for unauthorized disclosure of unclassified controlled nuclear information.

**b) Identify the topics that should be included in an initial briefing.**

Initial briefing content should include the following:

- Overview of the DOE facility's/organization's mission
- Overview of the facility's/organization's major S&S program responsibilities
- Access control
- Escort procedures
- Protection of Government property and badge procedures
- Identification of controlled and prohibited articles
- Protection of unclassified controlled information
- Procedures for reporting incidents of security concerns (e.g., attempts to gain unauthorized access to classified information or matter)
- Identification of classification markings

**11. Safeguards and security personnel acting in personnel security shall demonstrate a familiarity-level knowledge of classified visit activities.**

**a) Discuss the security principle that serves as a basis for the Control of Classified Visits Program.**

"Need to know" is the principle used to ensure that only persons with the appropriate access authorizations receive access to classified information or matter in connection with visits involving the release or exchange of classified information or matter.

**b) Describe the process by which a DOD employee is approved to visit a DOE contractor site when the visit involves an exchange of secret restricted data and weapon data.**

*Restricted Data (RD) Visits by DOD and NASA Employees*

Access to RD is contingent upon submission of a DOE F 5631.20; NASA Form 405, Request for Access Approval; or a memorandum or electronic message signed by or in the name of the certifying official. The request must be forwarded for approval or other action to the Departmental element with jurisdiction over the information to which access is requested. The approving official must have the authority to approve such access.

Requests for access must include

- names, citizenship, dates of birth, and social security numbers of persons requesting access and organizations represented (if not Armed Services, relationship to DOD or NASA);
- facility and information to which access is requested (access to critical nuclear weapon design information must be specified as requested);
- security clearance or access authorization status of each person, including clearance date;
- purpose of visit and certification that each person needs the access in the performance of duty;
- anticipated date of visit and names of persons to be visited (if a conference is involved, the date, place, and sponsor of the conference must be specified);
- a certification that the matter to which access is requested relates to aeronautical and space activities (for requests from NASA).

**12. Safeguards and security personnel acting in personnel security shall demonstrate a working-level knowledge of the programs described in the following DOE Orders and manual:**

- **DOE O 470.1, Chapter IV, Safeguards and Security Awareness Program**
- **DOE O 470.1, Chapter VIII, Control of Classified Visits Program**
- **DOE O 472.1C, Personnel Security Activities**
- **DOE M 472.1-1B, Personnel Security Program Manual**

Note: DOE O 470.1, Chapter IV, Safeguards and Security Awareness Program, DOE O 470.1, Chapter VIII, Control of Classified Visits Program, DOE O 472.1C, Personnel Security Activities, and DOE M 472.1-1B, Personnel Security Program Manual have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-5, Personnel Security, and DOE M 470.4-7, Safeguards and Security Program References.

**a) Describe the general requirements for determining level of access authorization and investigative requirements.**

A Q access authorization must be requested when the duties of the position require access to any of the following:

- Top Secret or Secret Restricted Data
- Top Secret Formerly Restricted Data
- Top Secret National Security Information

- Classified information or matter designated as "COMSEC," "CRYPTO," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15
- SNM designated as Category I, and other categories with credible roll-up to Category I

Note: A Q access authorization also authorizes the individual access to the categories/levels of classified information or matter listed below for L clearances.

An L access authorization must be requested when the duties of the position require access to any of the following:

- Confidential Restricted Data
- Secret or Confidential Formerly Restricted Data
- Secret or Confidential National Security Information
- SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) require a Q access authorization

**b) Discuss the elements for processing personnel security cases.**

The elements for processing personnel security cases consist of screening and analysis.

*Screening*

When an investigative report is received, a personnel security specialist must review it to ensure that the required DOE scope of investigation for the particular type of access authorization has been met and that all derogatory and mitigating information has been identified.

Background Investigations (Initial Investigations or Reinvestigations). The investigative report must be reviewed to ensure that thorough information is provided on the individual's residence, employment, education, and military service, and that checks of references, credit, and law enforcement have been completed.

All derogatory and mitigating information, as well as any missing elements of investigative coverage, must be documented with the date and signature of the reviewer. Under certain circumstances, it is appropriate to proceed with adjudication even if information is missing. The individual's employer, as listed on the SF 86, must be checked against the employer as reported in the investigation to ensure they are identical; if not identical, a check will be conducted to determine if the reported employer (i.e., the current employer) has submitted a request for access authorization and if it has been approved for the same type of access authorization.

Cases for which the investigation is complete and no derogatory information has been reported must be appropriately documented If the reviewer has been delegated authority in writing to grant an access authorization, the granting must be so noted in the file. At least 5 percent of such cases must be reviewed by a senior personnel security specialist to ensure the investigation is, in fact, complete and contains no derogatory information. Such verification of review will be documented by the date and signature of the reviewer on the File Summary Sheet (DOE F 5631.16) or equivalent.

National Agency Checks. Individuals screening these investigations must determine whether all items have been covered. Derogatory and mitigating information must be listed and documented with the date and signature of the screener.

*Analysis*

Only DOE employees who are so authorized in writing may determine an individual's access authorization eligibility or render other formal determinations that affect an individual's access authorization status. (Note: This requirement does not preclude a contractor from having an employee execute a "Security Termination Statement" or restricting an employee's access to classified information or matter, or SNM, before notifying the DOE cognizant security authority.) DOE employees authorized to render access authorization eligibility determinations must receive training in the DOE personnel security process prior to actually rendering such determinations.

Favorable and unfavorable investigative information must be analyzed according to the criteria found in 10 CFR 710.8. Frequently, the reported derogatory information alone raises a security concern, but may be resolved when considered with other reported mitigating information.

When information contained in investigative reports or the receipt of other reliable information raises a question concerning an individual's eligibility for an access authorization, additional actions may be authorized for collecting relevant information pertaining to the eligibility determination. If the question is favorably resolved, the access authorization may be granted, continued, or reinstated. If the question cannot be favorably resolved, the individual's access authorization eligibility must be determined under 10 CFR 710. Additional actions may be required to adjudicate a case. If one of these actions is necessary, the approval for such action must be by a senior personnel security specialist other than the specialist making the recommendation.

If an investigation is complete, the authorized DOE employee may grant or continue an access authorization based on the existing record if

- the file is clear of derogatory information
- the post-investigative record fully mitigates any derogatory information
- an interview and/or other supplementary fact-finding effort has resolved all security concerns documented in the record

DOE's final determination regarding the eligibility for an access authorization will be provided in writing or electronically to the employer or prospective employer who initiated the request. This information may also be furnished to representatives of DOE contractors or to federal agencies having an official interest in the individual. If there is reason to notify the individual in writing of the final determination, such as at the completion of the administrative review process, as defined in 10 CFR 710, or at the granting of an interim access authorization, the notification will be in the form of a letter or memorandum, but no official DOE form reflecting the granting of an access authorization will be enclosed.

If it is determined by the DOE cognizant security authority that reported information falls within one or more of the categories in 10 CFR 710.8 and the case cannot be resolved locally, then the access authorization must be suspended or recommended for denial. A duplicate of the PSF, a summary statement, and a request for authority to initiate

administrative review processing under 10 CFR 710 must be transmitted to the Director, Office of Security. The individual's employer, any other Departmental element having an access authorization interest in the individual, and any other federal agency for which the individual holds an access authorization, security clearance, or SCI approval, or to which DOE has certified the individual's access authorization, must be notified immediately of the suspension action. The Central Personal Clearance Index (CPCI) must also be immediately updated and the individual's badging office notified.

Any case may be referred to the Director, Office of Security, for review and advice. Any case referred must reflect the rationale and recommendations for further action.

**c) Describe the processes used for screening and analysis of investigative results in personnel security cases, and methods for determining access authorization eligibility.**

See element "b" above.

**d) Discuss the requirements for interim access authorizations.**

Only under exceptional circumstances and when such action is clearly consistent with the national interest will an individual, before completion of the appropriate investigation, be permitted to have access to classified information or matter, or SNM, or be allowed to occupy a federal position designated by the cognizant personnel office as Critical-Sensitive. In all such cases, Interim Access Authorizations (IAAs) to Restricted Data, National Security Information, or SNM, or waivers of pre-appointment investigations, must be considered temporary measures pending completion of the investigation, which must be in process. The use of IAAs must be kept to the absolute minimum and considered only when properly requested in accordance with procedures in DOE M 470.4-5. An IAA to Restricted Data, National Security Information, or SNM must be approved by the Director, Office of Security. A waiver of a pre-appointment investigation must be approved by the Secretary. Individuals who are dual citizens or non-U.S. citizens must not be processed for IAAs.

**e) Describe when a "Data Report on Spouse" form must be filed.**

Access authorization applicants and holders must provide two completed copies of DOE F 5631.34, Data Report on Spouse/Cohabitant, directly to the processing personnel security office within 45 working days of marriage or cohabitation. Note: A cohabitant is a person who lives with the individual in a spouse-like relationship or with a similar bond of affection, but is not the individual's legal spouse, child, or other relative (in-laws, mother, father, brother, sister, etc.).

**f) Describe the requirements and processes of access authorization for foreign nationals, dual citizens, and naturalized U.S. citizens.**

*Foreign Nationals*

Where there are compelling reasons in furthering the DOE mission, foreign nationals (to include immigrant aliens) with a special expertise that is not possessed to a comparable degree by an available U.S. citizen may be granted access authorization only for specific programs, projects, contracts, licenses, certificates, or grants for which the individual needs

access to classified information or matter, or SNM. Such individuals will not be eligible for access to any greater level of classified information than the U.S. Government has determined may be releasable to the country of which the individual is currently a citizen, and such limited access may be approved only if the prior 10 years of the individual's life can be appropriately investigated. Additional lawful investigative procedures must be fully pursued to allay any doubts concerning the granting of access. A request to process a foreign national for an access authorization must be approved by the Departmental element with jurisdiction over the program where the individual will be employed, the Office of General Counsel, and the Office of Security before submission for investigation. A foreign national granted an access authorization must not receive access to the following types of classified information or matter:

- Top Secret, CRYPTO, or COMSEC information, except classified keys used to operate secure telephone units (STU IIIs)
- Intelligence or Special Access Program (SAP) information
- Information that has not been determined to be releasable by a U.S. Government Designated Disclosure Authority to the country of which the individual is a citizen;
- NATO Information
- Information for which foreign disclosure has been prohibited in whole or in part (identified as NOFORN)
- Classified information furnished by a third-party government, and information provided to the U.S. Government in confidence by a third-party government (identified as FGI)

*Dual Citizens*

Individuals who possess a dual citizenship (i.e., who are simultaneously a citizen of the U.S. and another country) and who have exercised citizenship rights in the foreign country, or have represented themselves as citizens of the foreign country, or who have intentions to do so in the future, must meet the requirements for foreign nationals given above. There are two alternatives to being processed as foreign nationals, as described below:

- Renunciation of the Citizenship in the Other Country. If the individual is willing to renounce citizenship in the other country, the individual must provide a notarized statement attesting to the fact that the non-U.S. citizenship has been formally renounced, and if available, evidence that the renunciation has been formally accepted by an official representative of the other country's government. Copies of documents completed by the individual to formally renounce non-U.S. citizenship must accompany the notarized statement. An individual's statement of renunciation must be considered invalid if the individual continues to exercise citizenship rights in a foreign country.
- Waiver. The DOE cognizant security authority, or the Director, Office of Security, for Headquarters cases, may waive the requirement to renounce the non-U.S. citizenship if it is determined that it would be detrimental to the individual or to DOE security objectives, or that the risk associated with the individual maintaining the non-U.S. citizenship status has been adequately mitigated. A copy of the security evaluation documenting this waiver must be maintained in the individual's PSF.

**g) Discuss the extensions, transfers, terminations, and reinstatements of access authorizations.**

Extension of an access authorization is the process that allows an individual to hold concurrent active access authorizations under the cognizance of two or more Departmental elements, two or more employers, or one employer under two or more contract numbers.

Transfer of an access authorization requires a personnel security office to accept the active access authorization granted by another personnel security office simultaneously with the termination of that access authorization by the latter.

Terminations. Within 2 working days of receipt of notification that an individual no longer requires access to classified information or matter, or SNM, DOE must terminate the individual's access authorization.

- An access authorization must be terminated when there is termination of employment or change of official duties so that the position no longer requires access to classified information or matter, or SNM. Continuation may be authorized by the processing personnel security office when the employer has certified that the individual will be reemployed or reassigned to a position that requires an access authorization within 3 months and that DOE will be kept informed of the individual's status. If an individual is cleared for more than one contract, each access authorization requires a separate termination action.
- The access authorization must be terminated if the holder is on leave of absence or extended leave and will not require access for at least 90 working days. (This includes leave for foreign travel, employment, or education not involving official U.S. Government business.) This 90-day period may be adjusted at the discretion of the DOE cognizant security authority or the Director, Office of Security.

Reinstatements. A new or updated and recertified SF 86 must be obtained if more than six months have elapsed since termination of the access authorization and more than one year has elapsed since the date of the previous form, or when any significant changes are known to have occurred since that date. When an SF 86 is not required, a request for reinstatement must contain the date of birth of the individual to establish positive identification. A new DOE F 5631.18 must be obtained in all cases.

**h) Describe the reinvestigation program.**

Except as authorized by the Director, Office of Security, individuals with access authorizations must be periodically reinvestigated. Reinvestigations are designed to ensure that individuals with access authorizations are periodically reevaluated to determine their continued need for such access authorizations and reinvestigated to determine their continued eligibility. A reevaluation and reinvestigation must be completed every 5 years for individuals holding Q access authorizations, and every 10 years for individuals holding L access authorizations.

**i) Discuss the requirements for the Personnel Security Assurance Program.**

Title 10 CFR 712, Human Reliability Program, consolidated the Personnel Security Assurance Program (PSAP) and the Personnel Assurance Program into a single program. The PSAP no longer exists.

**j) Discuss the requirements of the Safeguards and Security Awareness Program.**

S&S awareness programs must include

- an initial briefing for all DOE federal and contractor employees;
- comprehensive, refresher, and termination briefings for all federal and contractor employees and personnel granted DOE access authorizations;
- appropriate awareness briefings for any non-DOE personnel granted unescorted access to Departmental security areas (e.g., regarding information on prohibited articles).

**k) Discuss the requirements of the Classified Visits Program.**

Line management must establish local procedures for the control of classified visits. Procedures must ensure

- verification of the visitor's identity, programmatic "need to know", and that the visitor's clearance or access authorization is at least equal to the classification of the information to which access is being requested.
- identification of limitations and enforcement of controls for access to classified information or matter or facilities, and submission of appropriate forms, requests, etc., to the cognizant security authority and programmatic line management within the timeframes below.
    - Visit requests must be submitted at least 15 working days before the date of a one-time visit or the first day of a recurring visit.
    - Exceptions to required processing times will be allowed only for emergency visits (i.e., when visits must take place as a matter of urgency and importance and the processing lead time cannot be met). Emergency visits will only be approved as one-time visits.
    - Requests for visits/access to weapons programs, nuclear materials production facilities, or sensitive nuclear materials production information must be referred to the Associate Administrator for Defense Nuclear Security.
    - Requests for visits/access to uranium enrichment plants or facilities engaged in uranium enrichment technology development, including advanced isotope separation technology, must be referred to the Office of Nuclear Energy, Science and Technology.
    - Requests for access to Naval Nuclear Propulsion facilities must be referred to the Deputy Administrator for Naval Reactors.
- continuing visitor access approval is necessary for individuals who frequently visit DOE facilities. However, the access approval cannot exceed a period of one year or the final day of a contract for contractors, whichever is less. The approval may be renewed annually (at least every 12 months).
- operational approval of visits.
- maintenance of documentation associated with all classified visits/access.

- referral of any nonroutine, written, or visual material resulting from classified visits and proposed for public release to the Director, Public Affairs.
- limiting the sending and receiving of a classified visit request to the security office of OGAs.

**13. Safeguards and security personnel acting in personnel security shall demonstrate the ability to assess the personnel security program as described in the following DOE orders and manual:**

- **DOE O 470.1, Chapter IV, Safeguards and Security Awareness Program**
- **DOE O 470.1, Chapter VIII, Control of Classified Visits Program**
- **DOE O 472.1C, Personnel Security Activities**
- **DOE M 472.1-1B, Personnel Security Program Manual**

**a) Assess Department of Energy (DOE) or contractor strategies for maintaining the minimum number of access authorizations consistent with operational efficiency.**

**b) Assess the effectiveness of management and operating contractor preprocessing checks conducted in accordance with Department of Energy Acquisition Regulations (DEAR).**

**c) Assess contractor compliance with requirements for timely reporting of access authorization terminations to the Department of Energy (DOE).**

**d) Assess DOE personnel security staff capability to effectively adjudicate information contained in reports of investigation, personnel security interviews, and Department sponsored mental evaluations.**

**e) Assess DOE procedures for developing security investigation funding estimates in response to budget calls.**

**f) Assess the completeness/compliance factors of Personnel Security Assurance Program plans approved by field office managers.**

**g) Assess the effectiveness of procedures implemented by the DOE Headquarters and field offices to approve/process requests for classified visits.**

**h) Assess DOE field office and Headquarters compliance with the intent of the requirements/guidance of the Safeguards and Security Awareness Program.**

Elements "a" through "h" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**14. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of nuclear materials within the Department of Energy.**

**a) Using a list of nuclear materials, identify the classification (special nuclear material, source, or other) of the material.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

### b) Describe the categories of nuclear materials within the DOE.

*Category*

A category is a designation of the significance of nuclear materials that is based on the material types, the material forms, and the amount of material. The designation of nuclear materials consists of categories I, II, III, and IV.

Determination of the category involves grouping materials by type, attractiveness level, and quantity. In many cases, the material category is determined directly from the table, Graded Safeguards, shown below.

**Graded Safeguards**

| | Attractiveness Level | Pu/U-233 Category (kg) | | | | Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg) | | | | All E Materials Category IV |
|---|---|---|---|---|---|---|---|---|---|---|
| | | **I** | **II** | **III** | **IV**[1] | **I** | **II** | **III** | **IV**[1] | |
| **WEAPONS** Assembled weapons and test devices | A | All | N/A | N/A | N/A | All | N/A | N/A | N/A | N/A |
| **PURE PRODUCTS** Pits, major components, button ingots, recastable metal, directly convertible materials | B | ≥2 | ≥0.4< 2 | ≥0.2<0.4 | <0.2 | ≥5 | ≥1<5 | ≥0.4<1 | <0.4 | N/A |
| **HIGH-GRADE MATERIALS** Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; $UF_4$ or $UF_6$ (≥50% enriched) | C | ≥6 | ≥2<6 | ≥0.4<2 | <0.4 | ≥20 | ≥6<20 | ≥2<6 | <2 | N/A |
| **LOW-GRADE MATERIALS** Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); $UF_4$ or $UF_6$ (≥20% < 50% enriched) | D | N/A | ≥16 | ≥3<16 | <3 | N/A | ≥50 | ≥8<50 | <8 | N/A |
| **ALL OTHER MATERIALS** Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233[2] (any form, any quantity) | E | N/A | N/A | N/A | Reportable Quantities | N/A | N/A | N/A | Reportable Quantities | Reportable Quantities |

[1] The lower limit for Category IV is equal to reportable quantities in this Manual.

[2] The total quantity of U-233 = [Contained U-233 + Contained U-235]. The category is determined by using the Pu/U-233 side of this table.

### c) Describe the attractiveness levels of nuclear materials within the DOE.

*Attractiveness Level*

An attractiveness level is a categorization of nuclear material types and compositions that reflects the relative ease of processing and handling required to convert that material to a nuclear explosive device. See the Graded Safeguards table, above, for further information.

**15. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of nuclear material accountability practices.**

**a) Discuss the purpose of the following material control and accountability measurements:**
- **Accountability**
- **Verification**
- **Confirmatory**

*Accountability*

Accountability is the part of the Material Control and Accountability program encompassing the procedures and systems to
- perform nuclear material measurements
- verify the locations and quantities of nuclear materials through physical inventories
- maintain records and provide reports
- perform data analyses to account for nuclear material and to detect losses
- investigate and resolve apparent losses of nuclear material

*Verification*

Verification is a quantitative re-measurement of the amount of nuclear material in an item made to verify the quantity of nuclear material present. Verification measurements, when used to adjust accountability records, must have accuracy and precision comparable to, or better than, the original measurement method.

*Confirmatory*

A confirmatory measurement is a qualitative or quantitative measurement made to verify the integrity of an item by testing whether some attribute or characteristic of the nuclear material in the item is consistent with the expected attribute or characteristic of the material. The measurement method used for confirmatory measurements must be capable of determining the presence of a specific attribute of the material, consistent with valid acceptance and rejection criteria.

**b) Describe the three general types of measurement methods used to measure nuclear material.**

The site/facility operator must select, qualify, and validate measurement methods capable of providing the required levels of precision and accuracy. Target values for precision and accuracy of nuclear material measurements endorsed by recognized national and international nuclear organizations must be considered performance goals for facility measurement systems. Alternative measurement performance goals must be defensible and documented. Precision and accuracy requirements must be approved by the DOE cognizant security authority and documented in the MC&A plan. Procedures must be documented and implemented for each facility to ensure that only qualified measurement methods are used for accountability purposes.

The site/facility operator must develop, document, and maintain measurement methods for all nuclear material on inventory. These methods must be written to provide clear direction

to the analyst or operator, and must be validated initially and revalidated whenever changes are made.

- In determining inventory values, and consistent with the graded safeguards concept, measurement methods must be selected in a manner that minimizes the contribution of measurement error to the uncertainty of the inventory difference.
- Verification measurements, when used to adjust accountability records, must have accuracy and precision comparable to or better than the original measurement method.
- The method used for confirmatory measurements must be capable of determining the presence or absence of a specific attribute of the material consistent with valid acceptance and rejection criteria.
- All measurement methods must be calibrated using standard or certified reference materials or secondary standards traceable to the national measurement base, and must be revalidated as necessary.
- Measurement equipment and instruments must meet precision and accuracy requirements under in-plant conditions.
- Documentation of measurement data must be maintained to provide an audit trail from source data to accounting records.

**c) Discuss the following statistical terms:**

- **Random sample**
- **Standard deviation**
- **Measurement bias**
- **Random error**

*Random Sample*

A sample is a subset chosen from a population for investigation. A random sample is one chosen by a method involving an unpredictable component, in the sense that the selection of any element of the population is independent of the selection of any other element.

*Standard Deviation*

The standard deviation is the square root of variance. The formulas for standard deviation are:

Population or $\sigma^2 = \sqrt{\frac{\sum (x-\mu)^2}{N}}$ or Sample $S^2 = \sqrt{\frac{\sum (x-\bar{x})^2}{N-1}}$

Example:
The standard deviation for a group of children aged 5, 6, 8, and 9 is:

$$S = \sqrt{S^2} = \sqrt{\frac{\sum (x-\bar{x})^2}{N-1}} = \sqrt{2.5} = 1.58$$

*Measurement Bias*

Measurement bias, or systematic error, favors a particular result. A measurement process is biased if it systematically overstates or understates the true value of the measurement. For example, if a scale is not properly calibrated, it might consistently understate weight. In this

case, the measuring device — the scale — produces the bias. Human observation can also produce bias. The important thing to keep in mind is that biased measurements invariably produce unreliable results.

*Random Error*

Random error is the irreproducibility in making replicate measurements and affects the precision of a result. The distribution of random errors follows a Gaussian-shape "bell" curve. The precision is described by statistical quantities such as the standard deviation.

**d) Describe the key elements of a nuclear material accounting system.**

The facility nuclear materials accounting system must include checks and balances and must be structured to ensure timely detection of errors or discrepancies in records associated with a Category I or II quantity of SNM, including, where possible, detecting falsified data and identifying the responsible persons. Timeframes for detection of errors and discrepancies must be approved by the DOE cognizant security authority and documented in the MC&A plan. The system also must be capable of detecting omissions and other data discrepancies and ensuring completeness of accounting records.

**e) Describe the purpose for conducting the following physical inventories:**
- **Periodic physical inventories**
- **Special inventories**

*Periodic Physical Inventories*

Periodic physical inventories must be performed for each material balance area (MBA) according to the strategic importance of the material and the consequence of its loss.

Physical inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Process monitoring techniques may be used for material that is undergoing processing and recovery operations and is inaccessible for measurements. Plans and procedures must be developed and documented to define responsibilities for performing inventories and to specify criteria for conducting, verifying, and reconciling inventories. Statistical sampling, based on graded safeguards, may be used to verify the presence of items during inventories. Parameters for statistical sampling plans must be defined by the site/facility operator, and approved by the DOE cognizant security authority. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

*Special Inventories*

Procedures must be established and implemented for conducting special inventories at the request of authorized facility personnel, the DOE cognizant security authority, or as a result of routine disassembly of critical assemblies, changes in custodial responsibilities, missing items, inventory differences exceeding established control limits, and abnormal occurrences.

**f) Discuss the following physical inventory terms:**
- **Inventory difference**
- **Shipper/receiver difference**

*Inventory Difference*

Inventory difference is the difference between the nuclear material book inventory and the corresponding physical inventory adjusted for transfers in and out of the MBA. It is calculated using the following equation:

ID = BI - EI + TI - TO

where ID is the inventory difference; BI and EI are the beginning and ending inventories, respectively; and TI and TO are the transfers of nuclear material into and out of the MBA, respectively.

*Shipper/Receiver Difference*

The shipper/receiver difference is the difference between the measured quantity of nuclear material stated by the shipper as having been shipped and the measured quantity stated by the receiver as having been received.

**16. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of nuclear materials control within the DOE.**

**a) Describe the major containment areas required for nuclear materials within the Department.**

Security areas include PPAs, LAs, EAs, PAs, vital areas, MAAs, and specially designated security areas (e.g., Sensitive Compartmented Information Facilities [SCIFs] and Special Access Program Facilities [SAPFs]).

*Property Protection Areas*

PPAs are established to protect Government-owned property against damage, destruction, or theft. Protection may include physical barriers, access control systems, protective personnel or persons assigned administrative or other authorized security duties, IDSs, and locks and keys. The designation and description of PPA protective measures must be approved by DOE line management (e.g., SSP or SSSP). The requirements for PPAs must be configured to protect Government-owned property and equipment against damage, destruction, or theft, and must provide a means to control public access.

*Limited Areas*

LAs are security areas designated for the protection of classified matter and Category III quantities of SNM. LAs are defined by physical barriers encompassing the designated space and access controls to ensure that only authorized personnel are allowed to enter and exit the area. A means must be provided to detect unauthorized entry into the LA.

*Exclusion Areas*

EAs are security areas in which an individual's mere presence may result in access to classified matter. The boundaries of EAs must be encompassed by physical barriers. EAs require access controls that ensure only authorized personnel are allowed to enter and exit the area. Examples of means to detect unauthorized entry into the EA include PF patrols, closed circuit television systems, IDSs, or a combination of measures. Unauthorized entry into the EA must be detected.

*Protected Areas*

PAs are security areas used to protect Category II or greater quantities of SNM and to provide security zones surrounding separately defined MAAs. PAs must be encompassed by physical barriers that identify the boundaries, surrounded by a PIDAS, and equipped with access controls that ensure only authorized personnel are allowed to enter and exit.

*Vital Areas*

Vital areas are separate security areas that contain vital equipment within PAs. In addition to the protection strategies required for PAs, the following requirements must be applied:

- Boundaries must conform to the layered protection concept, with a separate vital area perimeter located within a PA.
- The perimeter must be monitored to deter and detect unauthorized entry attempts.
- Vital equipment must be protected with an IDS.
- Exits must be alarmed or controlled at all times.
- PF response time to an intrusion alarm must be less than the delay time that can be demonstrated from the time an alarm is activated at the PA boundary to task completion.
- All requirements for personnel and vehicle access control that apply to PAs apply to vital areas.

*Material Access Areas*

MAAs are security areas used to protect Category I quantities of SNM or credible roll-up quantities of SNM to a Category I quantity. MAAs must have defined boundaries with barriers that provide sufficient delay time to impede, control, or deter unauthorized access.

*Special Designated Security Areas*

Other areas with access restrictions include CASs, SASs, SCIFs, SAP facilities, local law enforcement agencies, or private alarm stations, secure communications centers, and automated information system centers.

**b) Discuss the function of each of the following nuclear material control programs:**

- **Access Control**
- **Surveillance**
- **Detection/assessment**

*Access Control*

A graded program must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment, the misuse of which could compromise the safeguards system.

*Surveillance*

A nuclear materials surveillance program must ensure that nuclear materials are in their authorized locations, be capable of detecting unauthorized activities or anomalous conditions, and be capable of reporting material status. The surveillance program must address both normal and emergency conditions and include periodic testing.

*Detection/Assessment*

Systems must be in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept. The system must be interfaced with the facility's physical protection and other organizational systems, as appropriate, and must be able to detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

**c) Discuss the key elements of the above nuclear material control programs.**

*Access Control Programs*

Following are key elements of access control programs:

- Materials Access. A documented program must be established and implemented for each facility to ensure that only properly authorized personnel have access to nuclear materials. This program must address procedures and mechanisms to detect and respond to access by unauthorized personnel. To minimize the potential for unauthorized access to nuclear material, the amount of material in use must be limited to that necessary for operational requirements, and excess material must be stored in repositories or kept in enclosures designed to ensure that access will be limited to authorized individuals.
- Data Access. Procedures must be established that ensure only authorized persons have the ability to enter, change, or access MC&A data and information.
- Equipment Access. Access must be controlled to data-generating and other equipment used in material control activities. Such equipment includes measurement equipment, data-recording devices, and tamper indicating devices (TIDs).
- Other Considerations. Access control programs must protect against unauthorized data and equipment modification, and must detect unauthorized activities during emergency or other unusual conditions.

*Surveillance Programs*

Surveillance procedures must describe the methodologies and operational/control points on which the program is based and provide for investigation, notification, and reporting of anomalies. Following are key elements of surveillance programs:

- Category I and II. Material surveillance programs for Category I and II quantities of SNM must ensure that materials are in authorized locations and that unauthorized material flows and transfers are detected. Category I locations must be evaluated to determine the ability of the material surveillance system to assess material losses from MAA and PA boundaries. Category II locations must be evaluated to determine the ability of the material surveillance system to assess material losses from the PA boundary. Material surveillance programs for all areas containing Category I or II quantities of SNM must include the following measures.
  - Only authorized and knowledgeable personnel who are capable of detecting incorrect or unauthorized actions can be assigned responsibility for surveillance of SNM.
  - Controls must be sufficient to ensure that a lone individual cannot gain access to a secure storage area.

- All persons in secure storage areas must be under constant surveillance (e.g., the two-person rule or equivalent surveillance) at any time the storage area is not locked and protected by an active alarm system.
- Surveillance must ensure that unauthorized or unaccompanied authorized personnel cannot enter the storage/processing area undetected when the door is unlocked or open.
- When items are outside an alarmed storage area within an MAA or PA, there must be a system of hardware, procedures, and administrative controls sufficient to ensure that unauthorized accumulation of a Category I quantity is detected. When the two-person rule is utilized as an administrative control, the two authorized persons assigned responsibility for maintaining direct control of the items must be physically located where they have an unobstructed view of each other and the items, and can positively detect unauthorized or incorrect procedures.
- SNM in use or process must be under material surveillance, under alarm protection, or, with the approval of the DOE cognizant security authority, protected by alternative means that can be demonstrated to provide equivalent protection.

- Category III. The material surveillance program for Category III quantities must ensure that when materials are not in locked storage, they are attended, are in authorized locations, and are not accessed by unauthorized persons.
- Category IV. The material surveillance program for Category IV quantities must be site-specific and approved by the DOE cognizant security authority.

*Detection/Assessment Programs*

Following are key elements of detection/assessment programs:

- TIDs. A documented program, administered by the MC&A organization, must be in place to control TIDs and ensure that TIDs are used to detect violations of container integrity. TID programs cannot be regarded as effective unless used in conjunction with a material surveillance program. Verification measurements rather than confirmation measurements must be used for Category III or greater items that are not under a material surveillance program. Testing of TID integrity, location, application, and the TID record system must be conducted.
- Portal Monitoring. The detection level of the SNM portal monitors must be based on the types and forms of SNM used, stored, or processed in the area and the credible number of removals associated with theft of a Category I quantity of SNM. Controls must be established to prevent unauthorized access to portal monitor instrumentation and cabling. A written response plan must be prepared and implemented to provide evaluation and resolution of all alarm conditions.
- Controls. Controls must be established to ensure detection equipment remains operational during emergency conditions. Detectors and calibration standards must be maintained and controlled to ensure that portal monitors are capable of meeting detection requirements. Periodic performance testing of portal monitors must be conducted.

- Waste Monitors. All liquid, solid, and gaseous waste streams leaving an MAA must be monitored to detect the theft or diversion of SNM. Facility waste monitoring equipment must be maintained and controlled to ensure that the equipment is capable of detecting specified amounts of SNM as determined by the DOE cognizant security authority. Instrumentation used to monitor waste and equipment removed from an MAA must be able to detect, in combination with other detection elements, the removal of a Category I quantity of SNM through a credible theft or diversion scenario. A response plan for evaluating and resolving situations involving any discharge exceeding facility-specific limits must be established by the site/facility operator for the facility, and approved by the DOE cognizant security authority.
- Daily Administrative Checks. Daily administrative checks must be implemented for each Category I MBA (or multiple MBAs where roll-up to a Category I quantity of SNM is credible). The DOE cognizant security authority must determine and approve the scope and extent of the checks and specify the detection objectives on the basis of recognized vulnerabilities.
- Other Detection/Assessment Mechanisms. MC&A systems must be established for monitoring and control to provide the capability of detecting and assessing unauthorized SNM removals. Systems can include weight sensors, SNM/physical presence detectors, fiber optic seals, surveillance cameras, vault monitors, emergency egress radiation monitors, real-time inventory locator systems, etc. The MC&A system must provide sufficient information to correctly assess the alarms, localize the removal, and estimate the quantity and form of the diverted or stolen material.

**17. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of the basic requirements of Material Control and Accountability as described in DOE O 474.1, Control and Accountability of Nuclear Materials and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-6, Nuclear Material Control and Accountability, and DOE M 470.4-7, Safeguards and Security Program References.

**a) Using the site material control and accountability plan, discuss the following requirements:**
- **Measurements and measurement control**
- **Planning and management**
- **Threat considerations**
- **Performance criteria**
- **Accounting system**
- **Physical inventories**
- **Control limits**
- **Loss detection elements**
- **Nuclear material alarms**
- **Nuclear material access control**
- **Containment**
- **Surveillance**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**b) Discuss the concept of defense-in-depth as it applies to material control and accountability.**

Defense-in-depth is the use of multiple, independent protection elements combined in a layered manner so that system capabilities do not depend on a single component to maintain effective protection against defined threats.

**c) Discuss the material control and accountability aspects of the site and facility emergency plans.**

Procedures must be established by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative. These measures must ensure that access to or removal of SNM would be detected during these periods. The MC&A plan must address control of SNM during emergency operations, and measures to be taken before resuming operations following an emergency.

**d) Explain the specific performance requirements for material control and accountability elements.**

Various documents, actions, and activities are approved by the DOE cognizant security authority. For each site/facility subject to the requirements of DOE M 470.4-6, a specific DOE cognizant security authority must be designated as the approving authority for these documents, actions and plans. Approval authorities may be delegated in writing to other DOE cognizant security authorities. The same official can be designated as the approving authority for more than one site/facility.

The site/facility operator must designate a management official to be responsible for the MC&A program. This official must be organizationally independent from responsibility for nuclear material utilization programs, including nuclear material production, storage, processing, research, and disposition. This official must have responsibility for, and the authority to ensure, the safeguards of accountable nuclear material, along with operations personnel.

A nuclear materials representative (NMR) must be designated for each site/facility with a reporting identification symbol (RIS). The NMR is to be responsible for nuclear materials reporting and data submission to the Nuclear Materials Management and Safeguards Systems (NMMSS).

**e) Explain how nuclear materials are categorized using material type, attractiveness levels, and material quantities.**

The material category of SNM locations (e.g., MBAs, MAA, PA, and facilities) must be determined to establish the required protection levels. In many cases, the material category is determined directly from the table, Graded Safeguards, below. Directions for determining the material category when multiple material types and attractiveness levels must be considered are provided in the following paragraphs. Determination of category involves

grouping materials by type, attractiveness level, and quantity. Material quantities are element weights for plutonium and isotope weights for uranium-235 (U-235) and uranium-233 (U-233). The following procedures are used for determining material category.

*One Material Type, One Attractiveness Level*

To determine the material category for one material type and one attractiveness level, sum the material in the attractiveness level and determine the category from the Graded Safeguards table.

*One Material Type, Multiple Attractiveness Levels (Where a Category III or Greater Quantity of B-Level Material is Included)*

To determine the material category for one material type and multiple attractiveness levels where a Category III or grater quantity of B-level material is included, complete the following steps:

- Determine the amounts of SNM for materials in each of attractiveness levels B, C, and D.
- Calculate the "effective" quantity for attractiveness levels B and C by multiplying the quantity in attractiveness levels B and C by the appropriate factors in the Effective Quantities table, below.
- Sum the effective amounts in attractiveness levels B and C.
- Compare the total effective amount, as calculated above, to the amounts in attractiveness level B from the Graded Safeguards table, below.
- Compare the amount of attractiveness level D to the Graded Safeguards table.
- The material category is the highest level of material category determined using the procedures above.

*One Material Type, Multiple Attractiveness Levels (Where Less than a Category III Quantity of B-Level Material is Included)*

To determine the material category for one material type and multiple attractiveness levels where less than a Category III quantity of B-level material is included, follow these steps:

- Determine the amounts of SNM for all attractiveness levels.
- Compare the total amounts in each level to those in the Graded Safeguards table.
- The material category level is the highest level of the material categories determined using the above procedures.

*Multiple Material Types*

To determine the material category for multiple material types, follow these steps:

- Determine the category for each material type following the above procedures.
- The category is that which is determined for the individual material type that requires the highest level of protection.

## Graded Safeguards

| | Attractiveness Level | Pu/U-233 Category (kg) | | | | Contained U-235/Separated Np-237/Separated Am-241 and -243 Category (kg) | | | | All E Materials Category IV |
|---|---|---|---|---|---|---|---|---|---|---|
| | | I | II | III | IV[1] | I | II | III | IV[1] | |
| **WEAPONS** Assembled weapons and test devices | A | All | N/A | N/A | N/A | All | N/A | N/A | N/A | N/A |
| **PURE PRODUCTS** Pits, major components, button ingots, recastable metal, directly convertible materials | B | ≥2 | ≥0.4< 2 | ≥0.2<0.4 | <0.2 | ≥5 | ≥1<5 | ≥0.4<1 | <0.4 | N/A |
| **HIGH-GRADE MATERIALS** Carbides, oxides, nitrates, solutions (≥25 g/L) etc.; fuel elements and assemblies; alloys and mixtures; $UF_4$ or $UF_6$ (≥50% enriched) | C | ≥6 | ≥2<6 | ≥0.4<2 | <0.4 | ≥20 | ≥6<20 | ≥2<6 | <2 | N/A |
| **LOW-GRADE MATERIALS** Solutions (1 to 25 g/L), process residues requiring extensive reprocessing; moderately irradiated material; Pu-238 (except waste); $UF_4$ or $UF_6$ (≥20% < 50% enriched) | D | N/A | ≥16 | ≥3<16 | <3 | N/A | ≥50 | ≥8<50 | <8 | N/A |
| **ALL OTHER MATERIALS** Highly irradiated forms, solutions (<1 g/L), uranium containing <20% U-235 or <10% U-233[2] (any form, any quantity) | E | N/A | N/A | N/A | Reportable Quantities | N/A | N/A | N/A | Reportable Quantities | Reportable Quantities |

[1] The lower limit for Category IV is equal to reportable quantities in this Manual.

[2] The total quantity of U-233 = [Contained U-233 + Contained U-235]. The category is determined by using the Pu/U-233 side of this table.

### Effective Quantities

| Attractiveness Level | Pu/U-233 Factor | U-235 Factor |
|---|---|---|
| B | 1 | 1 |
| C | ⅓ | ¼ |

### f) Discuss how materials categorization relates to the graded safeguards principle.

Under the graded safeguards concept, a safeguards program must provide the greatest relative amount of control and accountability for the types and quantities of SNM that can be most effectively used in a nuclear explosive device.

### g) Discuss how vulnerability assessments, performance testing, and performance requirements serve as loss detection elements.

*Loss Detection Evaluation*

An assessment program for identifying and evaluating facility capability to detect the loss of Category I quantities of SNM must be developed for each Category I facility. Potential targets must include all Category I and any other areas for which a credible scenario for unauthorized accumulation of a Category I quantity of SNM have been identified. VAs must

be approved by the DOE cognizant security authority and must be reviewed annually (at least every 12 months) and updated when there are system changes or when new information indicates a potentially significant change in the risk of unauthorized removal of SNM. Results of the reviews, including changes in the VAs, must be reflected in the vulnerability analyses reports.

*Performance Testing*

MC&A performance testing programs must be developed and documented to support and verify loss detection capability and system effectiveness. The scope and intent of performance testing must be based on the graded safeguards concept, i.e., the testing program demonstrates greater testing for higher category facilities than for lower category facilities. Performance tests must be designed to demonstrate that the MC&A system is functional and to ensure that the system performs as specified or required. In addition, the site/facility operator for the facilities must

- identify those system components that provide the greatest effectiveness against theft and diversion;
- design, conduct, and document tests that substantiate component effectiveness;
- integrate the results of these component tests into S&S risk management programs and VAs.

*MC&A Performance Requirements*

Specific performance requirements for selected MC&A system elements are established below. The performance of the selected system elements must be validated on a frequency documented in the MC&A plan. If system elements fail to meet the performance requirements, a corrective action plan must be developed and, where necessary, compensatory measures must be taken.

- Access Controls. Performance tests must be designed and conducted to fully evaluate the effectiveness of access controls for Category I and II quantities of SNM.
- Material Surveillance. Performance tests must be designed and conducted to fully evaluate the effectiveness of material surveillance activities for Category I and II quantities of SNM.
- TIDs. The TID record system must accurately reflect the location and identity of TIDs for at least 99 percent of the TIDs inspected. The TID program must ensure that TIDs are properly in place for at least 95 percent of the TIDs inspected.
- SNM and Metal Portal Monitoring. Performance testing requirements must include those necessary to verify VAs, detection requirements, and applicable tests described in ASTM International Standard Guides.
- Accounting Record Systems. The accounting record system must accurately reflect item identity and location for at least 99 percent of items selected. If more than 1 percent of the accounting records selected is found to be in error, corrective actions must be taken for the accounting system as a whole.
- Inventory Confirmation/Verification Measurements. For Category I and II items, acceptance/rejection criteria for verification measurements and, where possible, for confirmatory measurements, must be based on the standard deviation for the measurement method under operating conditions. Control limits for such criteria must be set at no wider than three times the standard deviation for the method. The control limits must be reviewed and approved by the DOE cognizant security authority.
- Inventory Difference Control Limits.

**h) Discuss the occurrence investigation and reporting requirements associated with material control and accountability.**

*Reporting Incidents of Security Concern*

The site/facility operator must identify MC&A loss detection elements for each MBA, and must establish a graded program for monitoring these elements and associated data to determine the status of nuclear material inventories and to identify security incidents. In addition, the DOE cognizant security authority must independently evaluate the significance of the incident. Information and actions related to loss detection, monitoring, and assessment activities must be documented and maintained.

**i) Discuss the administrative controls designed to prevent and detect material losses or diversions including internal reviews and assessment programs.**

*Loss Detection Evaluation*

An assessment program for identifying and evaluating facility capability to detect the loss of Category I quantities of SNM must be developed for each Category I facility. Potential targets must include all Category I and any other areas for which a credible scenario for unauthorized accumulation of a Category I quantity of SNM have been identified. VAs must be approved by the DOE cognizant security authority and must be reviewed annually (at least every 12 months) and updated when there are system changes or when new information indicates a potentially significant change in the risk of unauthorized removal of SNM. Results of the reviews, including changes in the VAs, must be reflected in the vulnerability analyses reports.

*Performance Testing*

MC&A performance testing programs must be developed and documented to support and verify loss detection capability and system effectiveness. The scope and intent of performance testing must be based on the graded safeguards concept, i.e., the testing program demonstrates greater testing for higher category facilities than for lower category facilities.

*MC&A Performance Requirements*

Specific performance requirements for selected MC&A system elements must be validated on a frequency documented in the MC&A plan. If system elements fail to meet the performance requirements, a corrective action plan must be developed and, where necessary, compensatory measures must be taken.

**18. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of materials accounting, as described in DOE O 474.1, Control and Accountability of Nuclear Materials and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-6, Nuclear Material Control and Accountability.

**a) Discuss how material accounting relates to the overall protection of nuclear material.**

*Access Controls*

A graded program must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment, the misuse of which could compromise the safeguards system. Following are key elements of access control programs:

- Materials Access. A documented program must be established and implemented for each facility to ensure that only properly authorized personnel have access to nuclear materials. This program must address procedures and mechanisms to detect and respond to access by unauthorized personnel. To minimize the potential for unauthorized access to nuclear material, the amount of material in use must be limited to that necessary for operational requirements, and excess material must be stored in repositories or kept in enclosures designed to ensure that access will be limited to authorized individuals.
- Data Access. Procedures must be established that ensure only authorized persons have the ability to enter, change, or access MC&A data and information.
- Equipment Access. Access must be controlled to data-generating and other equipment used in material control activities. Such equipment includes measurement equipment, data-recording devices, and TIDs.
- Other Considerations. Access control programs must protect against unauthorized data and equipment modification, and must detect unauthorized activities during emergency or other unusual conditions.

**b) Explain the specific requirements for the accounting system database, procedures, and accounts.**

*Accounting Systems*

A system for tracking nuclear material inventories, documenting nuclear material transactions, issuing periodic reports, and assisting with the detection of unauthorized system access, data falsification, and material gains or losses must be established and implemented. The accounting system must provide a complete audit trail for all nuclear material from receipt through disposition. The generally accepted accounting principles promulgated by the Financial Accounting Standards Board must be used in the design and operation of the nuclear material accounting system. Following are key elements of a nuclear materials accounting system:

- Accounting Systems Databases and Procedures. Procedures must be established and maintained that describe the structure and operation of the nuclear materials accounting system. The procedures must accurately reflect current nuclear material accounting practices. Specific requirements for accounting procedures must include
  - descriptions of the inventory database (including procedures for updating and reconciling inventory data with the results of physical inventories) and the required data elements for each applicable material type;
  - identification of accounting reports and their frequency, distribution, and timeliness, consistent with accounting requirement;
  - identification of organizational responsibilities for management and operation of the accounting system;
  - recording, reporting, and submitting data to the NMMSS by material type and reporting unit.

- Account Structure.
  - Facility nuclear material accounts must consist of one or more MBAs established to identify the location and quantity of nuclear materials in the facility. Readily retrievable accountability data must be maintained by the MBA and reflect quantities of nuclear materials inventory, quantities of nuclear materials received and shipped, and other adjustments to inventory.
  - The MBA account structure must sort data by material types, processes, and functions; provide the capability to localize inventory differences; and provide a system of checks and balances for verifying the accuracy of the accountability data and records.
  - An MBA boundary must not cross an MAA boundary. Each MBA must consist of a single geographical area and be an integral operation.
  - The site/facility operator must designate an MBA custodian for each MBA to ensure that MC&A requirements are implemented in that MBA.
  - The MBA custodian is responsible for controlling nuclear material located in the MBA, preparing and signing internal material transfer documents, and conducting and reconciling MBA physical inventories.
  - An MBA custodian must not be responsible for multiple MBAs when transfers of nuclear material occur between those MBAs (i.e., a single custodian must not serve as both shipper and receiver for material transfers).

**c) Describe the account structure for a facility.**

The facility nuclear materials accounting system must include checks and balances, and must be structured to ensure timely detection of errors or discrepancies in records associated with a Category I or II quantity of SNM, including, where possible, detection of falsified data and identification of the responsible persons. Timeframes for detection of errors and discrepancies must be approved by the DOE cognizant security authority and documented in the MC&A plan. The system also must be capable of detecting omissions and other data discrepancies and ensuring completeness of accounting records.

**d) Describe the required records and reports to be maintained by a facility.**

The site/facility operator must maintain records, submit data, and issue reports as required by M470.4-6 and facility procedures. The reports must accurately describe all nuclear material transactions and inventories. Inventory adjustments must be identified by the MBA and must be reported as required in M470.4-6.

Nuclear materials records must be updated by authorized personnel only. The records system must provide an audit trail for all transactions affecting the nuclear materials database. The records system must also be capable of generating electronic and/or hard copy book inventory listings of all SNM within 3 hours. The listing must differentiate between SNM and other nuclear material when necessary.

The accounting records system must be capable of being updated daily or on demand for all nuclear materials transactions. This requirement is for updating records based on reports or information; it does not pertain to how quickly a facility must be able to complete measurements.

**e) Discuss the process of conducting, verifying, and reconciling physical inventories.**

*Conduct of Physical Inventories*

Inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Process monitoring techniques may be used for material that is undergoing processing and recovery operations and is inaccessible for measurements. Plans and procedures must be developed and documented that define responsibilities for performing inventories, and must specify criteria for conducting, verifying, and reconciling inventories. Statistical sampling, based on graded safeguards, may be used to verify the presence of items during inventories. Parameters for statistical sampling plans must be defined by the site/facility operator and approved by the DOE cognizant security authority. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

*Physical Inventory Reconciliation Program*

A physical inventory reconciliation program must be implemented in which the book inventory for each MBA is compared with, and if necessary, adjusted to the physical inventory. The reconciliation must be completed within 15 calendar days following receipt of all inventory information, measurement data, and sample analyses. Any inventory differences must be identified and reported as required.

**f) Discuss the minimum required frequencies and special requirements for physical inventories by material category.**

Physical inventories must be performed for Category I and II MBAs that involve activities other than processing at a frequency determined by the DOE cognizant security authority, but at least semiannually (once every 6 months). The site/facility operator must ensure that physical inventories are performed bimonthly (once every two months) in Category I and II MBAs where processing occurs.

In processing areas where process controls provide equivalent levels of theft and diversion detection, physical inventories may be performed upon completion of the material campaign. In such cases, the DOE cognizant security authority must approve a processing plan before starting the campaign. The process plan must identify compositions and quantities of material to be processed, the projected processing timetable, the process control measures used, and procedures necessary for material controls during process interruptions. Other factors to be considered for frequency determination include personnel radiation exposure, the operational mode of the facility, and credible protracted diversion scenarios.

At least annually, each facility must perform a simultaneous physical inventory of all Category I and II MBAs for which the established inventory frequency is annual or more frequent. MBAs with extended inventory frequencies of greater than one year are excluded from this requirement.

Physical inventories for Category III and IV SNM MBAs must be performed at a frequency specified by the DOE cognizant security authority, but at least every two years (every 24 months).

Category IV source and other nuclear material in Category I and II MBAs must be inventoried at least every 2 years (every 24 months), except when the source and/or other nuclear material is a credible substitution material.

When source or other nuclear materials are credible substitution materials for SNM and are collocated with SNM, facilities must inventory substitution materials with the same frequency as the SNM and use inventory measurement methods that can distinguish between SNM, source, and other nuclear material. Except for materials required to be protected as SNM and potential substitution materials collocated with SNM, source and other materials outside Category I and II MBAs must be inventoried at a frequency approved by the DOE cognizant security authority and as documented in the MC&A plan.

In addition to the requirements listed above, inventory checks for Category IA items not in storage must be performed weekly for physical count verification, and monthly for serial number verification. Inventory checks for stored Category IA items must consist of a physical count whenever the storage area is accessed, and a monthly serial number verification.

**g) Discuss the purpose and use of inventory verification/confirmation measurements.**

*Inventory Verification/Confirmation Measurements*

A system for performing measurements as part of a physical inventory must be established and implemented by the site/facility operator for each MBA. Verification measurements must be made on SNM items that are not tamper-indicating. Confirmation measurements must be made on tamper-indicating SNM items. Such measurements may use a statistically based sampling plan applied in a manner consistent with the graded safeguards concept. The site/facility operator must develop sampling plans, which the DOE cognizant security authority must approve. These plans must be based on the defined population, and must not be a subset of the sample selected for physical inventory. Separate sampling plans must be implemented for verification and confirmation measurements to ensure that a sufficient number of non-tamper-indicating items are measured. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered. Minimum sampling parameters for safeguard categories are noted below.

**Minimum Sampling Parameters for Safeguard Categories**

| Category | Confidence Level | Minimum Detectable Defect |
|---|---|---|
| I | 95 percent | 3 percent |
| II | 95 percent | 5 percent |
| III & IV | 95 percent | 10 percent |

The site/facility operator must establish documented acceptance or rejection criteria for inventory confirmation and verification measurements based on valid technical and statistical principles. For Category I and II items, acceptance and rejection criteria must be consistent with performance requirements for confirmation and verification measurements. The site/facility operator must prepare and implement a response plan for evaluating and resolving all verification and confirmation measurements that fail to meet acceptance criteria. Items that fail to meet the confirmation or verification measurement acceptance criteria must not be processed before the discrepancy is resolved.

**h) Discuss the data quality assurance elements of the requirements for measurements and measurement control and how they are monitored to ensure continuing control of measurement errors.**

Measurement and measurement control programs approved by the DOE cognizant security authority must be implemented at all facilities with nuclear material. Measurement programs used to determine Category I or II inventories of SNM, or used to determine a Category I or II SNM throughput over a 6-month period, must meet the requirements set forth below. All measurement systems used for accountability purposes must have associated measurement control programs to ensure the quality of measurement data generated.

Measurement programs used to determine Category III or IV inventories of SNM must address the topics below, but the specific measurement and measurement control requirements will be determined by the DOE cognizant security authority.

Measurement systems used for accountability purposes must be precise and accurate enough to minimize the contribution of measurement error to the limit of error of the inventory difference. Nuclear materials not amenable to verification measurement must be identified in the facility's MC&A plan. Inventory values for these materials must be based on measured values or technically justified estimates. Justification and supporting documentation for these inventory values must be maintained and readily retrievable for review.

*Measurement Systems*

Nuclear material measurement systems must provide accurate nuclear material values for inventories and transactions.

- Sampling. Sampling programs must be implemented to ensure that portions of bulk material taken for measurement are representative of the bulk material. The site/facility operator must establish and implement a documented sampling plan for each measurement point used for accountability purposes. The plans must be based on valid technical and statistical principles and must take into account material type considerations. Sampling requirements include the following:
  - The basis for the sampling plan must be documented and validated through studies of the materials or items being sampled.
  - The sampling plan must specify, at a minimum, the sampling procedure, number and size of required samples, mixing time and procedure (when applicable), provisions for retaining archive samples, and estimates of variance associated with the sampling method.
  - Sampling procedures must be documented and reviewed annually (at least every 12 months) or whenever changes are made, including changes to the type or composition of the material being sampled.
- Measurement Methods. The site/facility operator must develop, document, and maintain measurement methods for all nuclear material on inventory. These methods must be written to provide clear direction to the analyst or operator, and must be validated initially and revalidated whenever changes are made. Requirements for measuring methods include the following:
  - In determining inventory values, and consistent with the graded safeguards concept, measurement methods must be selected in a manner that minimizes the contribution of measurement error to the uncertainty of the inventory difference.

- Verification measurements, when used to adjust accountability records, must have accuracy and precision comparable to or better than the original measurement method.
- The method used for confirmatory measurements must be capable of determining the presence or absence of a specific attribute of the material consistent with valid acceptance and rejection criteria.
- All measurement methods must be calibrated using standard or certified reference materials or secondary standards traceable to the national measurement base, and must be revalidated as necessary.
- Measurement equipment and instruments must meet precision and accuracy requirements under in-plant conditions.
- Documentation of measurement data must be maintained to provide an audit trail from source data to accounting records.

- Measurement Control Programs. The site/facility operator must develop and implement control programs for all measurement systems used for accountability purposes. Control programs must ensure the effectiveness of measurement systems and the quality of measured values used for accountability purposes. Control programs must also produce precision and accuracy values for use in determining inventory difference control limits and shipper/receiver limits of error.

**i) Discuss the measurement control programs used at a facility.**

See element "h," above.

**j) Discuss the requirements for the external material transfer program including the measurements and their time frames.**

Requirements for the external material transfer program are as follows:

- The shipper must obtain written verification and maintain documentation that the intended receiver is authorized to accept the material before the material is transferred.
- Transfers of nuclear material between facilities having a different reporting identification symbol (RIS) must be documented using the electronic equivalent of DOE/Nuclear Regulatory Commission (NRC) F 741. Manual/paper DOE M 741s may be used to meet this requirement with the approval of the DOE cognizant security authority. These forms must be prepared and distributed to the principals of the transaction and line management.
- Immediately after receipt, shipments must be subjected to a transfer check. Transfer checks must consist of confirming the shipping container or item count, validating the TID integrity and identification, verifying the tamper-indicating characteristics of the container, and comparing the shipment with shipping documentation to ensure it was received intact. For external transfers, all SNM containers must be tamper-indicating. For purposes of transfer checks, receipt occurs when the transfer vehicle is unloaded or the transfer vehicle's integrity is breached (TIDs removed or broken) at the receiving facility. The site/facility operator must have documented procedures that specify actions to be taken in the event discrepancies are detected. Records of transfer checks are subject to audit and must be retained at least until the next S&S survey. For accountability purposes, material in transit at the end of a reporting period must be included in the receiver's reported inventory even though physical receipt of the material has not yet occurred.

- For all unirradiated Category I and II quantities of SNM transferred between facilities having a different RIS, the receiver must perform a verification or accountability measurement unless both RISs are located on the same site and are operated by the same site contractor. Both verification measurements and accountability measurements are quantitative measurements used by the receiver to verify that the amount of SNM in a shipment is as stated by the shipper. Accountability measurements differ from verification measurements only in how they are used in the receiver's accountability system. Accountability measurements are entered in the receiver's accountability system as the value for the shipment. When verification measurements are used, the shipper's values are entered into the receiver's accountability records.
  - The receiver may choose to establish a new accountability value or accept and book the shipper's accountability value considering the potential impact on the inventory difference. Transfer of nuclear material produced to program specification and inherently tamper-indicating may be verified by performing a confirmatory measurement rather than a verification/accountability measurement unless the DOE cognizant security authority requires verification/accountability measurements. Use of confirmatory measurements in lieu of verification/ accountability measurements for such items requires a shipper/receiver agreement approved by both the shipper's and receiver's DOE cognizant security authority. For Category III and IV transfers, the DOE cognizant security authority may require that measurements be made consistent with the strategic, nonproliferation, and/or monetary value of the material, or as required for environmental, safety, and operational controls. Verification/accountability measurements must be completed prior to processing material, unless a deviation is approved. When verification/accountability measurements are required and materials are to be processed before the verification/accountability measurements have been made, the shipper and receiver must reach an agreement as to how significant shipper/receiver differences will be handled.
  - The shipper must independently determine the measured values before shipment unless the integrity of the item and of the existing measured values have been ensured. The shipper's measured values must be documented on DOE/NRC F 741.
  - The receiver's confirmation and verification/accountability measurements (when required) for Category I and II quantities of SNM transfers must be accomplished in accordance with the requirements. The receiver's verification/accountability measurements for transfers involving other categories of nuclear material, when required by the DOE cognizant security authority, must be performed in accordance with the requirements in the table given below.

## Shipper/Receiver Measurement Requirements

| Material Category and Attractiveness Level | Material Confirmation[1] | Verification/Accountability[2] Measurements |
|---|---|---|
| IA | 3 working days | Shipper's value |
| IB | 5 working days | 30 calendar days |
| IC, II | 10 working days | 30 calendar days |
| III | 10 working days | 120 calendar days or on input to process |
| IV | 20 working days | On statistical bases within 180 days or on input to process |

[1] Confirmatory measurement by nondestructive analysis, gross weight check, and item count (if not done as part of transfer checks). Confirmatory measurements are not required for all materials. When confirmatory measurements are required, they must be performed within the time frames of this table.

[2] Quantitative determination of material quantities (within designated measurement uncertainty limits). Accountability measurement values are entered into receiver's accountability records. For verification measurements, the shipper's values are entered into the receiver's accountability records. Verification/accountability measurements are not required for all materials. When verification/accountability measurements are required, they must be performed within the time frames of this table.

- For shipment of unirradiated SNM containing greater than 250 grams of a single SNM type and for each discrete item exceeding 250 grams, limits of error at the 95 percent confidence level must be assigned to shipper and receiver accountability/ verification measurements for both the element and isotope values. Limits of error need not be reflected on the DOE/NRC F 741 for external transfers when accountability measurements cannot be performed. For other shipments, the shipper and receiver may estimate the limits of error. Limits of error are also required for all measurements of external transfers of tritium that exceed 2 grams, except as noted above.
- Documented acceptance/rejection criteria must be established and used to evaluate confirmatory measurement data. A response plan for investigation and resolution of confirmatory measurements that fail acceptance criteria must be developed and implemented, and all anomalies must be investigated and resolved.
- If delays in completing the receiver's verification/accountability measurement will result in a protracted delay in closure of the transaction, a confirmatory measurement may be used to affect a "safeguards closure" of the transaction. The transaction is documented by an "A-S" entry on DOE/NRC F 741. A safeguards closure may be used when the integrity of the shipment is ensured and only verification/accountability measurement differences are possible between shipper and receiver. If the receiver's verification/accountability measurement performed after a safeguards closure indicates a shipper/receiver difference, the difference may be resolved by mutual agreement of the shipper and receiver with the approval of their DOE cognizant security authorities and an adjustment (correcting entry) to the DOE/NRC F 741, if required. The safeguards closure may be affected only when all of the following conditions have been met. No discrepancies are found in the verification of the piece count, identification number, integrity of the TIDs, and gross weight of the items or containers received, and no evidence indicating theft or diversion of the material is found. The shipper and receiver confirmation measurements must confirm the same nuclear material attribute, must compare results of the methods on a technically valid basis, and the results must be within the established limits of agreement.

Criteria for closing transactions, based on confirmatory measurements, are approved by both the shipper's and receiver's DOE cognizant security authority, and the shipper/receiver agreement is in effect for the transaction.
    - Limited processing is acceptable for materials not amenable to nondestructive assay in order to perform a receipt measurement, as approved by both the shipper's and receiver's DOE cognizant security authority. Limited processing can include homogenization and dissolution.
- SNM in foreign reactor fuel returns must either be measured, or the risk of diversion of material from the fuel must be documented, and the acceptance of the fuel without measurement must be approved by the responsible Under Secretary or his/her designee.

**k) Discuss the requirements for the internal material transfer program.**

Requirements for the internal material transfer program are as follows:

- The site/facility operator must provide a graded system of measurements and records to reflect the flow of material between MBAs within that facility and between it and other facilities on the same site.
- The facility control system must be designed to monitor transfer activities and to deter and detect unauthorized removal of material during transfers. It must flag abnormal situations (e.g., inappropriate transfers of quantities, materials, or unauthorized personnel receiving or shipping materials).
- Transfers must be documented on nuclear material transfer forms or electronic equivalents that contain required information, prepared and distributed within established time frames, and signed by authorized custodians or their alternates.
- Materials must be subjected to a transfer check within 1 work day after receipt. These checks must include verification of shipping container or item count, TID integrity (if applied), and identification number. These transfer checks must be compared with appropriate documentation. Irradiated SNM requires only a transfer check.
- When the isotope content of SNM transferred between MBAs is 50 grams (fissile) or more, the material must have a measured value before transfer. Measured values are not required for enriched uranium that is below 20 percent U-235 and below10 percent U-233. Confirmation/verification measurement requirements for internal transfers must be approved by the DOE cognizant security authority, including when measurements are not required.
- Acceptance/rejection criteria must be established and documented to evaluate measurement data for internal material transfers. In addition, procedures must specify notification and response requirements if nuclear material removal or another abnormal situation is detected.

**l) Discuss how material control indicators are analyzed and how an indicator is determined to be significant.**

The site/facility operator must develop and implement a program that is capable of detecting losses through evaluation and assessment of shipper/receiver differences, inventory differences, and other inventory adjustments. The program must assess the material control indicators described below and ensure detection of losses and unauthorized removal of

nuclear materials. Documented plans must specify responsibilities and procedures for evaluating material control indicators.

*Shipper/Receiver Difference Assessment*

Written procedures must be developed for evaluating shipper/receiver differences and for investigating and reporting significant shipper/receiver differences. A shipper/receiver difference is defined to be significant when it

- involves a discrepancy in the number of items, regardless of the quantity of nuclear material, or when confirmation measurements for the shipment fail to meet acceptance criteria covered in a shipper/receiver agreement.
- is statistically significant. The determination of whether a shipper/receiver difference is statistically significant is only required for those shipments for which verification/accountability measurements are made by both the shipper and receiver. A shipper/receiver difference is defined to be statistically significant when the magnitude of the difference exceeds either of the following:
  - the limit obtained by a statistical combination of the valid limits of error for the shipper's and receiver's measured values
  - the square root of two times a single valid limit of error when either the shipper's or receiver's limit of error is invalid (When both the shipper's and receiver's limits of error are determined to be invalid, the limits of error must be recalculated, and the statistical significance of the shipper/receiver difference must be reevaluated.)

Shipper/receiver difference data must be subjected to trend analysis to detect measurement bias or material loss. Analyses must be designed to detect statistically significant cumulative shipper/receiver differences and to trigger investigations when these differences are detected. The receiver must notify its DOE cognizant security authority and the shipper of any shipper/receiver difference determined to be significant. Both shipper and receiver must investigate their measurements and limits of error. Such investigations must be completed and documented. Shipper/receiver differences involving a discrepancy in number of items must be reported.

When shipper/receiver differences are determined to be statistically significant, but the quantities and strategic or monetary values are insufficient to warrant an investigation and subsequent correction to transfer documents, and when the receiver is DOE or one of its contractors or subcontractors, the difference need not be investigated and the party must record its own quantitative value. In the context of this paragraph, differences of less than 50 grams of fissile material or less than 5 grams of tritium are considered to be insufficient to require an investigation unless there are special circumstances. Authority to invoke the stipulations of this paragraph rests mutually with the shipper's and receiver's DOE cognizant security authority.

Statistically significant shipper/receiver differences may be resolved through any of the following methods:

- If both the shipper's and receiver's DOE cognizant security authorities obtain assurance that the measurements and limits of error are valid, and the investigation indicates that theft or diversion has not occurred, the shipper and receiver must record their own quantitative values.

- If either the shipper or receiver and their DOE cognizant security authority agree to accept the other's value, the shipper or receiver must prepare a corrected copy of the shipping document using the other's data.
- If the investigation does not result in a satisfactory resolution, the shipper/receiver difference must be resolved by the Departmental elements concerned through traditional DOE line management channels.

**m) Discuss the sampling methods used to determine physical inventory values.**

Sampling programs must be implemented to ensure that portions of bulk material taken for measurement are representative of the bulk material. The site/facility operator must establish and implement a documented sampling plan for each measurement point used for accountability purposes. The plans must be based on valid technical and statistical principles and must take into account material type, measurement requirements, and any special process or operational considerations.

The basis for the sampling plan must be documented and validated through studies of the materials or items being sampled. The sampling plan must specify, at a minimum, the sampling procedure, number and size of required samples, mixing time and procedure (when applicable), provisions for retaining archive samples, and estimates of variance associated with the sampling method. Sampling procedures must be documented and reviewed annually (at least every 12 months) or whenever changes are made, including changes to the type or composition of the material being sampled.

**n) Describe the weighing techniques used to determine physical inventory values.**

All scales and balances used for accountability purposes must be maintained in good working condition, recalibrated according to an established schedule, and checked for accuracy and linearity on each day that the scale or balance is used for accountability purposes.

**o) Describe the analytical methods used to determine physical inventory values.**

The site/facility operator must select, qualify, and validate measurement methods capable of providing the required levels of precision and accuracy. Target values for precision and accuracy of nuclear material measurements endorsed by recognized national and international nuclear organizations must be considered performance goals for facility measurement systems. Alternative measurement performance goals must be defensible and documented. Precision and accuracy requirements must be approved by the DOE cognizant security authority and documented in the MC&A plan. Procedures must be documented and implemented for each facility to ensure that only qualified measurement methods are used for accountability purposes.

**19. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of the material control processes as described in DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, and DOE M 470.4-6, Nuclear Material Control and Accountability.

**a) Discuss the requirements for controlling access to nuclear materials, data, and property.**

*Access Controls*

A graded program must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment, the misuse of which could compromise the safeguards system.

*Materials Access*

A documented program must be established and implemented for each facility to ensure that only properly authorized personnel have access to nuclear materials. This program must address procedures and mechanisms to detect and respond to access by unauthorized personnel. To minimize the potential for unauthorized access to nuclear material, the amount of material in use must be limited to that necessary for operational requirements, and excess material must be stored in repositories or kept in enclosures designed to ensure that access will be limited to authorized individuals.

*Data Access*

Procedures must be established that ensure only authorized persons have the ability to enter, change, or access MC&A data and information.

*Equipment Access*

Access must be controlled to data-generating and other equipment used in material control activities. Such equipment includes measurement equipment, data-recording devices, and TIDs.

*Other Considerations*

Access control programs must protect against unauthorized data and equipment modification, and must detect unauthorized activities during emergency or other unusual conditions.

**b) Discuss the requirements for each of the following containment boundaries including category considerations: protected areas, materials access areas; materials balance areas; storage repositories; and processing areas.**

*Materials Access Areas and Protected Areas*

Controls must be in place to ensure that Category I quantities of SNM are used, processed, or stored only within an MAA contained in a PA, and that Category II quantities of SNM are

used, processed, or stored only within a PA. The containment program must do the following:

- Identify authorized activities and locations for nuclear materials
- Identify mechanisms used to detect unauthorized activities
- Identify material types, forms, and amounts authorized to be removed from the MAA or PA
- Identify containment controls for normal and emergency conditions
- Require a periodic audit of the containment program to ensure compliance and system effectiveness
- Evaluate roll-up

*Material Balance Area*

Controls must be established and implemented for each facility to ensure that nuclear materials are used, processed, or stored within an MBA, and are controlled in accordance with the graded safeguards concept. These controls must ensure that materials are removed only through authorized pathways or portals, and that they are subject to transfer and verification procedures identified in M470.4-6. Controls for MBAs must be formally documented and must meet the following requirements:

- Identify geographical boundaries and functions of the MBA
- Identify material types, forms, and quantities permitted in each MBA
- Describe administrative controls for each MBA
- Define custodial responsibilities for nuclear materials contained within an MBA
- Identify personnel authorized to receive or ship nuclear material
- Identify material flow into and out of the MBA
- Ensure material transfer procedures are followed
- Ensure that material quantities transferred across MBA boundaries are based on measured values

*Processing Area*

Controls must be established for nuclear materials being used or stored in processing areas. The controls for in-process areas must do the following:

- Describe activities and locations for storing material
- Identify components used to detect unauthorized activities or conditions
- Include procedures for moving material into or out of the processing area
- Describe control procedures for normal and emergency conditions and for maintenance activities
- Describe response actions to be taken in abnormal situations
- Provide for audit of the processing controls on a periodic basis to ensure system effectiveness

**c) Discuss the graded requirements for the materials surveillance program.**

*Graded Protection*

The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for, or consequences of, all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft,

compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

**d) Discuss how each of the detection/assessment elements listed in the Order addresses the potential for theft or diversion of nuclear material.**

*Tamper Indicating Devices*

A documented program, administered by the MC&A organization, must be in place to control TIDs and ensure that TIDs are used to detect violations of container integrity. TID programs cannot be regarded as effective unless used in conjunction with a material surveillance program. Verification measurements rather than confirmation measurements must be used for Category III or greater items that are not under a material surveillance program. Testing of TID integrity, location, application, and the TID record system must be conducted.

*Portal Monitoring*

The detection level of the SNM portal monitors must be based on the types and forms of SNM used, stored, or processed in the area and the credible number of removals associated with theft of a Category I quantity of SNM. Controls must be established to prevent unauthorized access to portal monitor instrumentation and cabling. A written response plan must be prepared and implemented to provide evaluation and resolution of all alarm conditions.

*Controls*

Controls must be established to ensure detection equipment remains operational during emergency conditions. Detectors and calibration standards must be maintained and controlled to ensure that portal monitors are capable of meeting detection requirements.

*Waste Monitors*

All liquid, solid, and gaseous waste streams leaving an MAA must be monitored to detect the theft or diversion of SNM. Facility waste monitoring equipment must be maintained and controlled to ensure that the equipment is capable of detecting specified amounts of SNM as determined by the DOE cognizant security authority. Instrumentation used to monitor waste and equipment removed from an MAA must be able to detect, in combination with other detection elements, the removal of a Category I quantity of SNM through a credible theft or diversion scenario. A response plan for evaluating and resolving situations involving any discharge exceeding facility-specific limits must be established by the site/facility operator for the facility, and approved by the DOE cognizant security authority.

*Daily Administrative Checks*

Daily administrative checks must be implemented for each Category I MBA (or multiple MBAs where roll-up to a Category I quantity of SNM is credible). The DOE cognizant security authority must determine and approve the scope and extent of the checks and specify the detection objectives on the basis of recognized vulnerabilities.

*Other Detection/Assessment Mechanisms*

MC&A systems must be established for monitoring and control to provide the capability of detecting and assessing unauthorized SNM removals. Systems can include weight sensors, SNM/physical presence detectors, fiber optic seals, surveillance cameras, vault monitors, emergency egress radiation monitors, real-time inventory locator systems, etc. The MC&A system must provide sufficient information to correctly assess the alarms, localize the removal, and estimate the quantity and form of the diverted or stolen material.

**20. Safeguards and security personnel acting in material control and accountability shall demonstrate an expert-level knowledge of the administrative controls required to ensure the integrity and quality of Material Control and Accountability systems and procedures as described in DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-6, Nuclear Material Control and Accountability.

**a) Describe the content, review, and approval requirements for facility material control and accountability procedures.**

At a minimum, the MC&A plan must include

- the elements of the MC&A program that are designed to deter and detect loss, theft, and diversion of nuclear materials and the unauthorized control of a weapon, test device, or materials that can be used to make an improvised nuclear device;
- measures to ensure that nuclear materials are in their authorized locations and being used for their intended purposes;
- a description of the local implementation of DOE M 470.4-6, which must document how the MC&A program meets the requirements of DOE M 470.4-6;
- facility-specific requirements approved by the DOE cognizant security authority including, but not limited to, agreements between Government and contractor organizations, access control and material surveillance testing measures, and the scope and extent of the performance testing program;
- MC&A plan review frequency and change control mechanisms.

The MC&A plan must be approved by the DOE cognizant security authority.

**b) Assess the material control and accountability procedures for consistency with the approved material control and accountability plan.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**c) Describe the types of material control and accountability emergency procedures required.**

Procedures must be established by the site/facility operator for emergency conditions and periods when MC&A systems are inoperative. These measures must ensure that access to or removal of SNM would be detected during these periods. The MC&A plan must address control of SNM during emergency operations, and measures to be taken before resuming operations following an emergency.

**d) Assess the material control and accountability emergency procedures to ensure they are in compliance with DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**e) Assess the controls that limit access to the accounting system and nuclear materials accounting data.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**f) Describe the checks and balances required in the nuclear material accounting system.**

MC&A system checks and balances, including separation of responsibilities and duties, are used to identify irregularities and detect tampering with materials or MC&A system components.

**g) Assess the contractor's assessment program for integrity and quality of the material control and accountability system.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**h) Determine when a review is required of a new and existing facility.**

Reviews must be conducted and documented before startup of new facilities or operations and when changes occur in facilities, operations, or MC&A features that might alter the performance of the MC&A system.

**i) Discuss the periodicity of material control and accountability internal audits conducted by organizations independent of material control and accountability and the requirements for them.**

An organization independent of MC&A must conduct internal audits of the facility's MC&A function to assess compliance with internal plans and procedures. The frequency of these audits must be approved by the DOE cognizant security authority.

**21. Safeguards and security personnel acting in material control and accountability shall demonstrate a working-level knowledge of the documentation and reporting requirements for the national database as described in DOE O 474.1, Control and Accountability of Nuclear Materials, DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, and DOE M 474.1-2, Manual for Nuclear Materials Management and Safeguards System Reporting and Data Submission.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, and DOE M 474.1-2, Manual for Nuclear Materials Management and Safeguards System Reporting and Data Submission, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-6, Nuclear Material Control and Accountability.

**a) Discuss the documentation requirements for nuclear material transactions.**

All RIS-level nuclear materials transactions, material balances, and inventories must be documented and reported to the Nuclear Materials Management and Safeguards System (NMMSS), which is the national database for nuclear materials.

**b) Describe content and reporting frequency for material balance reports.**

A material balance report (MBR) must be prepared either by the NMMSS operator or by the facility. A facility may place a standing request with NMMSS to have an NMMSS-generated MBR, DOE/NRC F 742, provided to the facility in lieu of submission of reports. In such cases, the facility that receives the NMMSS-generated report must reconcile the facility's balances to the NMMSS. Reconciling transactions must be submitted if NMMSS balances are to be changed.

MBRs must be submitted annually, by September 30, for all facilities, and additionally as directed by the DOE cognizant security authority, or as specified in facility attachments or transitional facility attachments for DOE facilities selected under the provisions of the U.S./International Atomic Energy Agency (IAEA) Safeguards Agreement.

**c) Discuss the inventory reporting requirements for nuclear materials.**

The elements and isotopes that must be reported to NMMSS are shown in the table below. Weights must be reported in the metric weight units specified for each nuclear material as shown in the table. Both element and isotope weights are reported if they round to a reportable quantity. In cases where the element is a reportable quantity, but the isotope is not a reportable quantity, the material must still be reported, but for the isotope, the entry should be 0 (zero). In cases where the isotope is a reportable quantity, but the element is not a reportable quantity, the material must still be reported, but for the element, the entry should be 0 (zero).

## Nuclear Material Reporting Units and Characteristics

| Name of Material | MT Code | Reporting Weight Unit Report to Nearest Whole Unit | Element Weight | Isotope Weight | Isotope Weight % |
|---|---|---|---|---|---|
| Depleted Uranium | 10 | Whole Kg | Total U | U-235 | U-235 |
| Enriched Uranium | 20 | Whole Gm | Total U | U-235 | U-235 |
| Plutonium-242[1]<br>Americium-241[2]<br>Americium-243[2] | 40<br>44<br>45 | Whole Gm<br>Whole Gm<br>Whole Gm | Total Pu<br>Total Am<br>Total Am | Pu-242<br>Am-241<br>Am-243 | Pu-242<br>–<br>– |
| Curium | 46 | Whole Gm | Total Cm | Cm-246 | – |
| Californium<br>Plutonium<br>Enriched Lithium | 48<br>50<br>60 | Whole Microgram<br>Whole Gm<br>Whole Kg | –<br>Total Pu<br>Total Li | Cf-252<br>Pu-239+Pu-241<br>Li-6 | –<br>Pu-240<br>Li-6 |
| Uranium-233 | 70 | Whole Gm | Total U | U-233 | U-232 (ppm) |
| Normal Uranium<br>Neptunium-237<br>Plutonium-238[3]<br>Deuterium[4] | 81<br>82<br>83<br>86 | Whole Kg<br>Whole Gm<br>Gm to tenth<br>Kg to tenth | Total U<br>Total Np<br>Total Pu<br>$D_2O$ | –<br>–<br>Pu-238<br>$D_2$ | –<br>–<br>Pu-238 |
| Tritium[5]<br>Thorium<br>Uranium in Cascades[6] | 87<br>88<br>89 | Gm to hundredth<br>Whole Kg<br>Whole Gm | Total H-3<br>Total Th<br>Total U | –<br>–<br>U-235 | –<br>–<br>U-235 |

1 Report as Pu-242 if the contained Pu-242 is 20 percent or greater of total plutonium by weight; otherwise, report as Pu 239-241.
2 Americium and Neptunium-237 contained in plutonium as part of the natural in-growth process are not required to be accounted for or reported until separated from the plutonium.
3 Report as Pu-238 if the contained Pu-238 is 10 percent or greater of total plutonium by weight; otherwise, report as plutonium Pu 239-241.
4 For deuterium in the form of heavy water, both the element and isotope weight fields will be used; otherwise, report isotope weight only.
5 Tritium contained in water ($H_2O$ or $D_2O$) used as a moderator in a nuclear reactor is not an accountable material.
6 Uranium in cascades is treated as enriched uranium and should be reported as material type 89.

### d) Describe the data processing procedures required for submitting data to the nuclear materials management and safeguards system.

*Reporting to NMMSS*

Facilities must report data to the NMMSS electronically. If electronic means are unavailable, reporting using paper forms is permitted; however, it must be coordinated through the DOE cognizant security authority. Under emergency conditions or if a special, non-standard report is required, paper forms may be used. When a reportable quantity of an accountable nuclear material is recovered during deactivation, decommissioning, or decontamination, the recovered material must be reported to NMMSS, even when the material has been previously written off the NMMSS records. A DOE/NRC F 741 must be used. Facilities are encouraged to use the NMMSS software package, Safeguards Management of Software, to edit site data prior to submitting electronic data to NMMSS. This software may be obtained from the NMMSS operator.

*Units, Standards, Conversions, and Data Definitions*

Data reporting requirements include the following:

- Metric units are required for reporting information to the NMMSS.
- If weights are in pounds, the conversion factor 0.45359 kg/pound must be used.
- A year is defined as 365.2422 days.

- Nuclear material properties (e.g., half-lives) can be found online at www.nndc.bnl.gov. For other material properties and equations, see the CRC Handbook of Chemistry and Physics.
- Measurements that have been made and records that have been kept in volume units must be converted to the reporting unit for the material type. Material properties and equations in the CRC Handbook of Chemistry and Physics must be used to convert gas or liquid volumes to the appropriate units.
- Parts per million calculations will be recorded as follows:
  - ppmv for volume basis
  - ppm for mass basis
  - ppma for number of atoms basis
- The calculation for ppm of U-232 in total uranium is a mass basis.
- NMMSS will not accept slashes (\ and/), semi-colons (;), colons (:), question marks (?), or number signs (#). Do not use those characters when entering data.
- For the definitions of data elements, e.g., field length and whether a numeric or alpha character is allowed, see NMMSS Reports D-23 (for DOE) and D-24 (for NRC), available from the NMMSS operator.

*Rounding Policy*

Rounding policy requirements are as follows:

- Quantities will be reported with fractions of ½ or greater rounded upwards and fractions of less than ½ of a reporting unit reported as the number zero (0).
- Nuclear material transactions should be documented and reported as accurately as possible to reflect the actual quantity of material transferred. If a transaction of discrete items (each of which is less than a reportable quantity) sums to a reportable quantity, the transaction should be recorded to most accurately reflect the actual quantity involved. The shipper and receiver will decide how to ensure appropriate accounting documentation in NMMSS. Both the shipper and receiver must agree on the method to use. If the shipper and receiver cannot agree, the Office of Plutonium, Uranium, and Special Material Inventory will decide how best to document the transaction.
- When performing general calculations not related to discrete items in a transaction, do the calculation first before rounding.
- For software development purposes, sites or facilities may use more significant digits than noted in DOE M 470.4-6.

**e) Assess the contractor's documentation and reporting of nuclear materials transactions.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**22. Safeguards and security personnel acting in materials control and accountability shall demonstrate the ability to assess a program as described in DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

**a) Participate in a vulnerability assessment designed to identify and assess the capability for detecting loss of a Category I quantity of Special Nuclear Material.**

**b) Assess whether the contractor's performance testing program for material control and accountability meets the requirements of DOE O 470.1, Safeguards and Security Program.**

**c) Assess the contractor's programs and processes for occurrence investigation and reporting of material control and accountability related incidents.**

**d) Assess the facility's administrative controls that ensure the integrity and quality of systems and procedures for material control and accountability.**

**e) Assess the facility's nuclear materials accountability system that tracks nuclear material inventories, documents nuclear material transactions, issues periodic reports, and assists in detecting unauthorized system access, data falsification, and material gains or losses.**

**f) Audit the facility's physical inventory program for nuclear materials.**

**g) Assess the facility's graded program for controlling personnel access to: nuclear materials; data for nuclear materials accountability, inventory, and measurement; data generating equipment; and, other items/equipment where misuse or tampering could lead to compromise of the safeguards system.**

**h) Assess the contractor's graded surveillance program for monitoring nuclear materials, detecting unauthorized activities or anomalous conditions, and for reporting material and facility status.**

**i) Assess the contractor's capability to detect and assess the unauthorized removal of nuclear materials.**

Elements "a" through "i" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**23. Safeguards and security personnel acting in information security shall demonstrate a working-level knowledge of information security systems.**

**a) Describe the classification levels and categories.**

The three classification levels, in descending order of sensitivity and potential damage to the National security, are Top Secret, Secret, and Confidential:

- Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.
- Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- Confidential. The damage tests for restricted data/formerly restricted data (RD/FRD) and national security information (NSI) are different, as noted below:

- RD/FRD. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
- NSI. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.

The three classification categories are RD, FRD, and NSI:

- RD is information classified under the Atomic Energy Act that concerns the design, manufacture, or utilization of nuclear weapons; the production of special nuclear material; or the use of SNM in the production of energy. RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.
- FRD is information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.
- NSI is information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

**b) Describe the function of the following information security programs:**

- **Classified Matter Protection Control**
- **Operations Security**
- **Technical Surveillance Countermeasures**
- **Automated Information Systems Security**
- **Sensitive Unclassified Information**
- **Sensitive Compartmented Information and Foreign Intelligence Information**
- **Special Access Programs**

*Classified Matter Protection Control*

The function of classified matter protection control is

- to protect and control classified matter that is generated, received, transmitted, used, stored, reproduced, or destroyed;
- to establish an audit trail for all accountable classified matter;
- to establish required controls based on classification level (Top Secret, Secret, or Confidential) and category (RD, FRD, or NSI) or special handling instructions or caveats.

*Operations Security*

The function of operations security is

- to help ensure that Critical Program Information (CPI), including unclassified controlled information, is protected from inadvertent and unauthorized disclosure;
- to provide management with the information required for sound risk management decisions concerning the protection of sensitive information;
- to ensure that Operations Security (OPSEC) techniques and measures are used throughout the Department.

*Technical Surveillance Countermeasures*

Information on technical surveillance countermeasures can be found in Section E of DOE M 470.4-4. This is an official use only (OUO) document and must be requested from the DOE Office of Security and Safety Performance Assurance.

*Automated Information Systems Security*

The automated information system or automated information system network must ensure that only personnel who are authorized to access C/FGI-MOD matter can access that information. For instance, networks interconnected with a public switched-broadcast network (e.g., the Internet) must provide precautions (e.g., authentication or file access controls) to ensure that C/FGI-MOD matter is protected against unauthorized access. C/FGI-MOD matter being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide protection (e.g., encryption) to ensure that the information is not improperly accessed.

*Sensitive Unclassified Information*

The function of the designation sensitive unclassified information is to adequately and consistently control and protect unclassified controlled information (UCI) within the Department. UCI is broadly defined as unclassified information that may be exempt from public release under the Freedom of Information Act and for which disclosure, loss, misuse, alteration, or destruction may adversely affect national security, governmental interests, or personal privacy.

*Sensitive Compartmented Information (SCI)*

The function of the designation sensitive compartmented information is to identify classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected in accordance with policy established by the Director, Central Intelligence.

*Foreign Intelligence Information (FII)*

Foreign intelligence information is national security information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, which carries the following special caveats for control and access:

- WNINTEL = Warning Notice — Intelligence Sources and Methods Involved
- NOCONTRACT = Not Releasable to Contractors/Consultants
- ORCON = Dissemination and Extraction of Information Controlled by Originator

*Special Access Programs*

A special access program is a program established for a specific class of classified information that imposes protection and access requirements that exceed those normally required for information at the same classification level.

**c) Discuss the Department's counterintelligence program and its relationship to the information security program.**

The information security program must be integrated with other programs such as S&S program planning and management, physical protection, PF, personnel security, and nuclear material

control and accountability. Additionally, the activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, intelligence, and counterintelligence programs should be considered in the implementation of DOE M 470.4-4.

**24. Safeguards and security personnel acting in information security shall demonstrate a working-level knowledge of the classified computer security program as described in the DOE directives:**

- **DOE O 471.2A, Information Security Program**
- **DOE M 471.2-2, Classified Information Security Systems Manual**

Note: DOE O 471.2A, Information Security Program has been cancelled. Therefore, some of the information provided in this competency statement was taken from DOE M 470.4-4, Information Security, and DOE M 470.4-7, Safeguards and Security Program References.

**a) Discuss the onsite management and planning activities for automated information systems security.**

This is a site specific competency.

**b) Discuss the assignment of automated information systems security responsibilities, authorities, and accountability.**

*Classified Information Systems Security Program Manager (ISPM)*

The ISPM is a DOE employee knowledgeable in information systems security and is appointed by the Director of the Office of Safeguards and Security (NN-51). The ISPM

- serves as the program manager for Classified Information Systems Security and ensures implementation of the Classified Information Systems Security Program within DOE;
- develops and recommends DOE policies, standards, procedures, and guidelines for protecting information systems that collect, create, process, transfer, store, or provide access to classified information;
- maintains a continuing review of DOE M 471.2-2 to ensure that current technology is being applied to the protection of information systems that create, process, store, transfer, or provide access to classified information, and to eliminate those practices that are no longer needed or effective;
- approves secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information;
- annually reviews and updates, as needed, the Periodic Risk Assessment for the DOE Classified Information Systems Security Program and the DOE Statement of Generic Threat to Automated Information Systems;
- in coordination with the field, designates the DAA for information systems that operate under the jurisdiction of more than one Headquarters and field element;
- reviews and concurs on accreditation for systems operating at Protection Level 5 or 6 that operate under the jurisdiction of one Headquarters or field element;
- represents the DOE before federal, private, and public organizations concerned with protecting classified information systems;
- reports changes in Information Systems Security Operations Manager (ISOM) and DAA appointments to all DAAs;

- coordinates
  - with the Unclassified Computer Security Program Manager;
  - with the Office of Energy Intelligence on the protection of Sensitive Compartmented Information (SCI);
  - implementation of the Classified Information Systems Security Program with Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, Materials Control and Accountability (MC&A), and other programs, as appropriate;
  - the development, publication, and distribution of guidelines for the protection of classified information systems;
- provides education, awareness, and training activities that
  - ensure that education in DOE's Classified Information Systems Security Program policies and practices is available to the ISOMs and Information Systems Security Site Managers (ISSMs) (scheduling of these educational activities must allow all ISOMs and ISSMs to participate within one year of their appointment);
  - maintain a capability to facilitate the electronic exchange of information systems security information, such as awareness alerts on sniffer attacks, viruses, etc.;
  - periodically present information systems security workshops;
  - periodically sponsor an Information Systems Security Program training conference;
- supports, maintains, and coordinates an advice and assistance capability for use by any ISOM or ISSM within DOE;
- maintains and coordinates an incident response capability to provide timely assistance and system vulnerability information to DOE sites;
- provides guidance for a technology development program to support the Classified Information Systems Security Program, and periodically briefs DAAs, ISOMs, and ISSMs on activities and results of the program;
- collects and disseminates information relevant to the Classified Information Systems Security Program;
- monitors the Classified Information Systems Security Program findings and deficiencies resulting from surveys, inspections, and reviews;
- conducts timely reviews of the system protection documentation and the certification for information systems located in Sensitive Compartmented Information Facilities (SCIFs) received from cognizant ISOMs, and provides comments to the Office of Energy Intelligence.

*Designated Approving Authority (DAA)*

The DAA is a DOE employee appointed by the Operations Office Manager. He/she is responsible for evaluating the protection measures in an information system as described in the Classified Information Systems Security Plan (ISSP), the results of any certification tests, the certification of the system, and any residual risks of operating the system. The DAA may designate additional tests that must be performed prior to meeting accreditation requirements. With this appointment, the operations manager provides the DAA with written authorization to accept the residual risks and responsibility for the loss of confidentiality, availability, and/or integrity of all classified information systems under DAA jurisdiction. The authorization must include accreditation, provisional accreditation, withdrawal of accreditation, and suspension of operations for all classified information systems with

operational boundaries fully contained under his/her jurisdiction. The ISOM may also be appointed as the DAA. The DAA

- serves as accrediting authority for each DOE and covered contractor classified information system with operational boundaries fully contained under his/her jurisdiction;
- ensures that DOE M 471.2-2 is implemented for each classified information system under his/her jurisdiction, that each system is accredited or reaccredited every three years (except for information systems that process SCI), and that the accreditation or reaccredidation is documented;
- ensures that the accreditation of each system under his/her jurisdiction is withdrawn, and that the system is properly sanitized when the system no longer processes classified information or when changes occur that might affect accreditation;
- ensures that DAA authorities are delegated only to DOE employees who are knowledgeable in information systems security;
- reports any changes in ISOM or ISSM appointments to the ISPM.

*Classified Information Systems Security Operations Manager(s) (ISOM)*

The ISOM is a DOE employee that is knowledgeable in information systems security and appointed by the operations office manager. The ISOM must participate in ISPM-sponsored training in the Classified Information Systems Security Program within one year of his/her appointment. The ISOM

- communicates appropriate incident reports received from sites to the ISPM;
- ensures periodic review of the Classified Information Systems Security Program consistent with the Operations Office Survey Program at each site under the jurisdiction of the DOE operations office;
- evaluates information systems for accreditation and provides results to the DAA;
- monitors responses to findings and other deficiencies identified in surveys, inspections, and reviews of each site's Classified Information Systems Security Program to ensure that any necessary corrective or compensatory actions have been completed;
- coordinates
  - the Classified Information Systems Security Program with the Unclassified Information Systems Security Program;
  - implementation of the Classified Information Systems Security Program with requirements of other DOE programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and MC&A programs.

*Classified Information Systems Security Site Manager(s) (ISSM)*

The ISSM is appointed by the site manager to be responsible for implementation of the site Classified Information Systems Security Program. A separate ISSM may be appointed for information systems in an SCIF if the site determines that another ISSM is needed. In this capacity, the ISSM also functions as the site point of contact for all classified information systems security issues. The ISSM

- ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users which must include, but is not limited to, various combinations of self-paced and formal classes, security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids;

- ensures the development, documentation, and presentation of information systems security training for escorts in information systems operational areas;
- establishes, documents, implements, and monitors the Classified Information Systems Security Program for the site, and ensures site compliance with DOE requirements for information systems;
- ensures the development of procedures for use in the site Classified Information Systems Security Program;
- identifies and documents unique threats to information systems at the site;
- ensures that the site's Classified Information Systems Security Program is coordinated with the SSSP or the SSP;
- coordinates
  - implementation of the site Classified Information Systems Security Program with the other site programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and MC&A;
  - development of a site self-assessment program for the Classified Information Systems Security Program;
  - self-assessment of the site's Classified Information Systems Security Program, which is to be performed between operations office surveys;
- ensures the development of site procedures to
  - govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;
  - ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;
  - report classified information systems security incidents;
  - require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems and classified information;
  - detect malicious code, viruses, and intruders (hackers);
  - review and approve ISSPs, certification test plans, and certification test results;
- determines, using guidance from the data custodian(s), the appropriate levels of concern for confidentiality, integrity, and availability for each information system that processes classified information;
- certifies to the DAA, in writing, that each ISSP has been implemented, that the specified protection measures are in place and properly tested, and that the classified information system is functioning as described in the ISSP;
- recommends to the DAA, in writing, approval or disapproval of the ISSP test results and the certification statement;
- ensures that the DAA is notified when a system no longer processes classified information or when changes occur that might affect accreditation;
- participates in ISPM-sponsored information systems security training within one year of his/her appointment;
- ensures that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system.

*Classified Information Systems Security Officer(s) (ISSO)*

The ISSO

- ensures implementation of security measures for each classified information system for which he/she is responsible;
- identifies and documents any unique threats to classified information systems for which he/she is the ISSO and forwards them to the ISSM;
- if so directed by the DAA and/or if an identified unique local threat exists, performs a risk assessment to determine if additional countermeasures beyond those identified in DOE M 471.2-2 are required;
- develops and implements a certification test plan for each classified information system for which he/she is the ISSO, as required by this DOE M 471.2-2 and the DAA;
- prepares, maintains, and implements an ISSP that accurately reflects the installation of protection measures for each classified information system for which he/she is responsible;
- maintains the record copy of the ISSP and related documentation for each classified information system for which he/she is the ISSO;
- notifies the DAA (through the ISSM) when a system no longer processes classified information, or when changes occur that might affect accreditation;
- ensures that
  - the sensitivity level of the information is determined prior to use on the classified information system and the proper security measures are implemented to protect this information;
  - unauthorized personnel are not granted use of, or access to, a classified information system;
  - formal access controls are implemented for each classified information system, except stand-alone personal computers and stand-alone workstations;
- documents any special protection requirements identified by the data custodians and the protection measures implemented to fulfill these requirements for the information contained in the classified information system;
- ensures that confidentiality, integrity, and availability levels of concern are determined for each classified information system for which he/she is responsible;
- implements site procedures to
  - govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;
  - ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;
  - report classified information systems security incidents;
  - require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for protecting classified information systems and classified information;
  - detect malicious code, viruses, and intruders (hackers);
  - review and approve ISSPs, certification test plans, and certification test results;
- ensures that users are properly trained in system security by identifying classified information systems security training needs (including system-specific training) and personnel who need to attend system security training programs;

- conducts ongoing security reviews and tests of classified information systems to periodically verify that security features and operating controls are functional and effective;
- evaluates proposed changes or additions to the classified information systems and advises the ISSM of their security relevance.

*Classified Information Systems Application Owner/Data Custodian*

The application owner/data custodian

- determines and declares the sensitivity level of information prior to the information being processed, stored, transferred, or accessed on the classified information system;
- advises the ISSO of any special protection requirements for information to be processed on the classified information system;
- determines and documents the data and application(s) that are essential to fulfill the site mission, and ensures that requirements for contingencies are determined, implemented, and tested;
- ensures that information is processed on a classified information system that is accredited at a level sufficient to protect the information.

*Users of Classified Information Systems*

Users of classified information systems must

- comply with the Classified Information Systems Security Program requirements;
- be aware of and knowledgeable about their responsibilities in regard to classified information systems security;
- be accountable for their actions on a classified information system;
- ensure that any authentication mechanisms (including passwords) issued for the control of their access to classified information systems are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access;
- acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information;
- participate in training on the information system's prescribed security restrictions and safeguards before receiving initial access to a system, and as a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

**c) Discuss the required contents and maintenance of an automated information systems security plan.**

The automated information system or automated information system network must ensure that only personnel who are authorized for access to C/FGI-MOD matter can access that information. For instance, networks interconnected with a public switched-broadcast network (e.g., the Internet) must provide precautions (e.g., authentication or file access controls) to ensure that C/FGI-MOD matter is protected against unauthorized access. C/FGI-MOD matter being transmitted over broadcast networks like the Internet, where unauthorized access is possible, must provide protection (e.g., encryption) to ensure that the information is not improperly accessed.

**d) Perform an evaluation of the automated information systems security plan to verify its currency and conformity with DOE orders.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**e) Describe the local statement of threat to computing and information resources.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**f) Describe how the automated information systems security organization interfaces with the configuration management and planning processes.**

Configuration management (CM) ensures that protection features are implemented and maintained in the system. CM applies a level of discipline and control to the processes of system maintenance and modification. CM provides system users with a measure of assurance that the implemented system represents the approved system. Maintenance changes that affect the security of the system must receive a configuration management review. All security-relevant modifications must be subject to the provisions of the system configuration management program.

**g) Describe how the automated information systems security organization interfaces with the site risk management program.**

Risk management is a process that considers the prevailing DOE threat analysis, the effect of countermeasures applied to the processing environment, the remaining vulnerability of the processing environment (residual risk), and the protection requirements and value of the information being processed. Countermeasures are increased until the risk is reduced to an acceptable level or until the cost of reducing the risk becomes prohibitive. If the DAA determines that the remaining risk is not acceptable, management must then determine if the automation requirements are sufficient to justify additional costs.

Risk management balances the data custodian's perceived value of the information and his/her assessment of the consequences of loss of confidentiality, integrity, and availability against the costs of protective countermeasures and day-to-day operations. DOE's risk management process includes

- threat analysis;
- risk analysis that evaluates generic threats, technologies, and architectures and integrates associated findings into DOE directives governing information systems;
- data custodians' declarations of the consequences of loss of confidentiality, integrity, and availability;
- site program implementation that evaluates the unique concerns of the site (i.e., threats, protective technologies, procedures, etc.) and integrates those concerns with site operations;
- system implementation that identifies, evaluates, and integrates the impact of information loss, system vulnerabilities, data custodian protection requirements, cost of protective measures, and mission requirements;

- system operation where the remaining risk (residual risk) is accepted and oversight is initiated to ensure that the level of residual risk is managed throughout the information system's life cycle.

**h) Describe the automated information systems security awareness program and the automated information systems security organization's responsibilities for that program.**

The ISSM is responsible for ensuring the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users. This training and awareness program must include, but is not limited to, various combinations of classes (both self-paced and formal), security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids.

**i) Discuss the integration of TEMPEST considerations into automated information systems security planning.**

TEMPEST is a short name referring to the investigation, study, and control of compromising emanations from telecommunications and automated information systems equipment.

**j) Describe the local automated information systems security inspection/review program.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**k) Describe the purpose and methodology of certification and accreditation of computing resources.**

The certification and accreditation process begins after protection measures have been implemented and any required classified information system protection documentation has been approved. The certification process confirms that the protection profile described in the ISSP has been implemented and that the protection measures are functioning properly. This process culminates in an accreditation for the system to operate.

*Certification Process*

The certification process confirms that the system's protection measures have been correctly implemented in accordance with the selected protection profile.

- Independent Validation and Verification. For information systems intended to operate in Protection Level 5 or 6, an Independent Validation and Verification (IV&V) review must be conducted and funded by the cognizant site.
- Sensitive Compartmented Information. For information systems located in an SCIF that processes SCI, the cognizant ISSM, ISOM, and ISPM must review the information system protection documentation and the certification of the information system. Once they have completed their review, they send it, with their comments, to the Office of Energy Intelligence and the Office of Nonproliferation and National Security.

*Accreditation*

The DAA must review and accredit all systems before they become operational to ensure they maintain the confidentiality, availability, and integrity of all classified information.

*Provisional Accreditation*

The DAA may grant provisional accreditation (temporary authority) to operate an information system because of incomplete documentation or to permit a major conversion of the information system. Provisional accreditation may be granted for up to 180 days. DAA-approved protection measures must be in place and functioning during the period of provisional accreditation.

*Reaccreditation*

As outlined in National Policy contained in OMB Circular A-130, Management of Federal Information Resources, and National Security Telecommunications and Information Systems Security Directives (NSTISSDs), each information system must be reaccredited every three years or whenever security-significant changes are made to the accredited information system. The ISSO/ISSM/ISOM must review proposed modifications to information systems to determine if the proposed modifications will impact the protections on the system. If the protection aspects of the systems environment change, if the applicable protection requirements change, or if the protection mechanisms implemented for the system change, the system must be reaccredited. During the reaccredidation cycle, the DAA may choose to grant an interim accreditation for the system.

*Withdrawal of Accreditation*

The DAA must evaluate the risks and consider withdrawal of accreditation if the protection measures approved for the system do not remain effective or whenever any of the following items change: levels of concern, protection level, technical or nontechnical protection measures, vulnerabilities, operational environment, operational concept, or interconnections. The DAA must withdraw accreditation and ensure proper sanitization when the system is no longer required to process classified information, or if the operational need for the system no longer outweighs the risk of operating the system.

*Invalidation of an Accreditation*

An accreditation becomes invalid immediately whenever detrimental, security-significant changes occur to any of the following: the required protection level, the operational environment, the operational concept/mission, or the interconnections.

*Certification and Accreditation of Multiple Systems*

If two or more similar information systems are to be operated in equivalent operational environments (e.g., the levels of concern and protection level are the same and the physical security requirements are similar), the ISSO may write and the DAA may approve a Master ISSP to cover all such information systems. The information systems covered by a Master ISSP may range from personal computers up to and including multi-user information systems and local area networks that meet the criteria for a Master ISSP approach. The Master ISSP must conform to the ISSP requirements in DOE M 471.2-2 and specify the information required for each certification for an information system to be accredited under the plan.

Information Systems Certification Report (ISCR). The ISCR must contain the information system's identification, the information system's location, and a statement signed by the ISSM certifying that the information system implements the requirements in the Master ISSP.

The DAA must accredit the first information system under the Master ISSP. The ISSM must certify that all other individual information systems to be operated under the Master ISSP meet the conditions of the approved Master ISSP. This certification, in effect, accredits the individual information systems to operate under the Master ISSP. A copy of each certification report must be retained with the approved copy of the Master ISSP.

Recertification of Information Systems. All information systems certified under a Master ISSP remain certified until the Master ISSP is changed or three years have elapsed since the information system was certified. If either the levels of concern or the protection level described in the Master ISSP changes, all information systems certified under the Master ISSP must be recertified.

**l) Describe the methods used to protect information assets on computing resources.**

*Clearing and Sanitization*

Clearing. All internal memory, buffer, or other reusable memory must be cleared to effectively deny access to previously stored information. Detailed instructions on clearing must be issued periodically by the ISPM.

Sanitization. Classified information systems resources must be sanitized before they are released from classified information controls or released for use at a lower classification level. Detailed instructions on sanitization must be issued periodically by the ISPM.

*Examination of Hardware and Software*

Information systems hardware and software must be examined when received from the vendor and before being used.

Information Systems Software. Commercially procured software must be tested to ensure that it contains no obvious features that might be detrimental to the security of the information system. Security-related software must be tested to ensure that the security features function as specified.

Information Systems Hardware. The equipment must be examined to determine that it appears to be in good working order and has no "parts" that might be detrimental to the secure operation of the information system when placed under site control and cognizance. Subsequent changes and developments that affect security may require additional examination.

*Identification and Authentication Management*

Identification and authentication are required to ensure that users are associated with the proper security attributes, such as identity, protection level, or location. Controls, such as biometrics or smart cards, may be used at the discretion of the ISSO with approval of the ISSM and DAA.

- Identifier Management. User identifiers must be managed in accordance with documented procedures.
- Authenticator Management. User authenticators must be managed in accordance with documented procedures.

- Unique Identification. Each user must be uniquely identified and that identity must be associated with all auditable actions taken by that individual.
- Authentication at Logon. Users must be required to authenticate their identities at "logon" time by supplying their authenticator, such as a password, smart card, or biometrics, in conjunction with their user identification (ID) prior to the execution of any application or utility on the system.
- Access to Authentication Data. Access to authentication data must be restricted to authorized personnel through the use of encryption, file access controls, or both.
- User ID Reuse. Prior to reuse of a user ID, all previous access authorizations (including file accesses for that user ID) must be removed from the system.
- User ID Removal. When an employee leaves the sponsoring organization or loses access to the system for cause, that individual's user ID and authentication must be removed or disabled from the system.
- User ID Revalidation. All active user IDs must be revalidated at least annually and information such as sponsor and means of off-line contact (e.g., phone number, mailing address) must be updated as necessary.
- Protection of Authenticator. An authenticator in the form of knowledge (password) or possession (smart card, keys) must not be shared with anyone.
- Protection of Passwords. When passwords are used as authenticators, the following must apply:
  - Passwords must be protected at a level commensurate with the classification level and most restrictive classification category of the information to which they allow access.
  - Passwords must contain a minimum of six nonblank characters.
  - Passwords must be generated by a method approved by the DAA. Password acceptability must be based on the method of generation, the length of the password, and the size of the password space. The password generation method, the length of the password, and the size of the password space must be documented. In no case must a user develop his/her own password.
  - When an information system cannot prevent a password from being echoed (e.g., in a half-duplex connection), an overprint mask must be printed before the password is entered to conceal the typed password.
  - User software, including operating system and other security-relevant software, comes with a few standard authenticators (e.g., System, Test, Master) and passwords already enrolled in the system. Passwords for all standard authenticators must be changed before allowing the general user population access to the information system. These passwords must be changed after a new system version is installed or after other action is taken that might result in the restoration of these standard passwords.
  - If the level of concern for confidentiality is low, the lifetime of a password must not exceed 12 months. If the level of concern is medium or high, the lifetime of a password must not exceed 6 months.

**m) Describe the methods used to provide physical protection of computing resource assets.**

*Protection*

The information and system must be located in a security area appropriate to the classification and sensitivity of the data.

*Visual Access*

Devices that display or output information in human-readable form must be positioned so as to deter unauthorized individuals from reading the information without the knowledge of the user.

*Information Protection*

Information must be protected in accordance with DOE site requirements.

*Unescorted Access*

All personnel granted unescorted physical access to the system must have an appropriate security clearance and a "need to know" or a presumptive "need to know" for all information on the information system.

**n) Discuss the continuity and reliability of critical operations for computing resources.**

The manager or supervisor directly responsible for the system must determine the need for continuity of operations or develop a contingency plan for each information system. This decision must be documented and signed by the manager or supervisor. A statement of the decision and the basis for that decision must be documented in the ISSP, including if a continuity of operations plan or contingency plan is not needed.

Documented procedures for the backup of all essential information, software, and documentation must be implemented on a regular basis. The backup procedures must be attached to or referenced in an attachment to the ISSP. The frequency of backups must be defined by the ISSO, with the assistance of the data custodian(s), and documented in the backup procedures.

**25. Safeguards and security personnel acting in information security shall demonstrate a familiarity-level knowledge of the requirements for information security as described in DOE Order 5639.8A, Security of Foreign Intelligence Information and Sensitive Compartmented Information.**

**a) Discuss the purpose and scope of DOE Order 5639.8A, Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities.**

*Purpose*

The purpose of DOE Order 5639.8A is to establish responsibilities and authorities for protecting foreign intelligence information (FII) and sensitive compartmented information facilities (SCIFs) within DOE.

*Scope*

The provisions of this Order apply to all Departmental elements and contractors performing work for the Department as provided by law and/or contract and as implemented by the appropriate contracting officer.

**b) Describe the interrelationship of the following:**
- **Foreign Intelligence Information**
- **Sensitive Compartmented Information**
- **Other information security programs**

*Foreign Intelligence Information (FII)*

FII is national security information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, which carries the following special caveats for control and access:
- WNINTEL = Warning Notice — Intelligence Sources and Methods Involved
- NOCONTRACT = Not Releasable to Contractors/Consultants
- ORCON = Dissemination and Extraction of Information Controlled by Originator

*Sensitive Compartmented Information (SCI)*

SCI is classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

*Other Information Security Programs*

Special Access Programs (SAPs) are any programs established under Executive Order 12356 or the Atomic Energy Act of 1954, as amended, that impose additional controls governing access to classified information involved with such programs beyond those required by normal management and safeguarding practices. These additional controls may include, but are not limited to, access approval, adjudication or investigative requirements, special designation of officials authorized to determine a "need to know," or special lists of persons determined to have a "need to know."

**c) Discuss the contents and use of DOE Procedural Guide — Security of Foreign Intelligence Information and Sensitive Compartmented Information and Facilities.**

The DOE Procedural Guide — Security of Foreign Intelligence Information and Sensitive Compartmented Information and Facilities implements the appropriate portions of Director of Central Intelligence Directives (DCIDs).

**d) Explain how Director of Central Intelligence Directives are utilized by Field elements.**

DCIDs are provided to DOE field elements for reference only. The applicable portions of these documents are or will be incorporated in Orders or procedural guides as appropriate.

**e) Discuss the goals, direction, and related duties and responsibilities with respect to the national intelligence effort as set forth in Executive Order 12333, "United States Intelligence Activities."**

The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense, and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal. Maximum emphasis should be given to fostering analytical competition among appropriate elements of the Intelligence Community.

All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council. A balanced approach between technical collection efforts and other means should be maintained and encouraged.

Special emphasis should be given to detecting and countering espionage and other threats and activities directed by foreign intelligence services against the United States Government, or United States corporations, establishments, or persons.

To the greatest extent possible consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, all agencies and departments should seek to ensure full and free exchange of information in order to derive maximum benefit from the United States intelligence effort.

**f) Discuss the requirements for safeguarding National Security Information as described in Executive Order 12958, "National Security Information."**

*General Restrictions on Access*

A person may have access to classified information provided that a favorable determination of eligibility for access has been made by an agency head or the agency head's designee, the person has signed an approved nondisclosure agreement, and the person has a "need to know" the information.

Classified information shall remain under the control of the originating agency or its successor in function. An agency shall not disclose information originally classified by another agency without its authorization. An official or employee leaving agency service may not remove classified information from the agency's control.

Classified information may not be removed from official premises without proper authorization.

Persons authorized to disseminate classified information outside the executive branch shall assure the protection of the information in a manner equivalent to that provided within the executive branch.

Consistent with law, directives, and regulation, an agency head or senior agency official shall establish uniform procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute,

disseminate, process, or store classified information have controls that prevent access by unauthorized persons and ensure the integrity of the information.

Consistent with law, directives, and regulation, each agency head or senior agency official shall establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

Consistent with directives issued pursuant to this order, an agency shall safeguard foreign government information under standards that provide a degree of protection at least equivalent to that required by the government or international organization of governments that furnished the information. When adequate to achieve equivalency, these standards may be less restrictive than the safeguarding standards that ordinarily apply to United States "Confidential" information, including allowing access to individuals with a "need to know" who have not otherwise been cleared for access to classified information or who have not executed an approved nondisclosure agreement.

Except as provided by statute or directives issued pursuant to this order, classified information originating in one agency may not be disseminated outside any other agency to which it has been made available without the consent of the originating agency. An agency head or senior agency official may waive this requirement for specific information originated within that agency. For purposes of this section, the Department of Defense shall be considered one agency.

**g) Describe the purpose, goals, and objectives of the Information Security Oversight office Directive No. 1 with regard to National Security Information.**

The Information Security Oversight Office, National Archives and Records Administration, published this Directive as a final rule and pursuant to Section 5.1(a) and (b) of Executive Order 12958, as amended, relating to classified national security information. The Executive order prescribes a uniform system for classifying, safeguarding, and declassifying national security information. It also establishes a monitoring system to enhance its effectiveness. This directive sets forth guidance to agencies on original and derivative classification, downgrading, declassification, and safeguarding of classified national security information.

**26. Safeguards and security personnel acting in information security shall demonstrate an expert-level knowledge of the requirements for control of Top Secret, Secret, and Confidential documents as described in the DOE orders listed below.**

- **DOE O 471.2A, Information Security Program**
- **DOE M 471.2-1, Classified Matter Protection and Control Manual**

Note: DOE O 471.2A, Information Security Program, and DOE M 471.2-1, Classified Matter Protection and Control Manual, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-4, Information Security, and DOE M 475.1-1A, Identifying Classified Information.

**a) Discuss classification levels and categories and the degree of control required for each.**

The three classification levels, in descending order of sensitivity and potential damage to the national security, are Top Secret, Secret, and Confidential:

- Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.
- Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- Confidential. The damage tests for RD/FRD and NSI are different, as noted below:
  - RD/FRD. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - NSI. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.

*Categories of Classified Information*

Categories of classified information are as follows:

- RD is information classified under the Atomic Energy Act that concerns the design, manufacture, or utilization of nuclear weapons; the production of special nuclear material; or the use of SNM in the production of energy. RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.
- FRD is information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.
- NSI is information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

**b) Describe the appropriate clearance level for access to each classification level.**

The following table, in accordance with the Atomic Energy Act, indicates the clearance level required for access to each classification level.

| Access Level | RD | FRD | NSI |
|---|---|---|---|
| Q | TS, S, C | TS, S, C | TS, S, C |
| L | C | S, C | S, C |

Legend:
RD= Restricted Data, FRD= Formerly Restricted Data, NSI= National Security Information
TS= Top Secret, S= Secret, C= Confidential

**c) Describe the proper storage of Top Secret matter not under personal control.**

Top Secret matter must be stored

- in a locked, General Services Administration (GSA)-approved security container with one of the following supplemental controls: (1) under IDS protection and by PF personnel responding within 15 minutes of alarm annunciation, or (2) with inspections by PF personnel occurring no less frequently than every two hours. If the container is located in an LA, EA, PA, or MAA, the GSA-approved security container must have a lock meeting federal specification FF-L-2740A, Locks, Combination.
- in a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.
- in a locked vault or VTR outside an LA, EA, PA, or MAA that must be under IDS protection. The PF must respond within five minutes of alarm annunciation.

**d) Describe the protection requirements for Top Secret matter in storage.**

Top Secret matter must be stored

- in a locked, GSA-approved security container with one of the following supplemental controls: (1) under IDS protection and by PF personnel responding within 15 minutes of alarm annunciation, or (2) with inspections by PF personnel occurring no less frequently than every two hours. If the container is located in an LA, EA, PA, or MAA, the GSA-approved security container must have a lock meeting federal specification FF-L-2740A, Locks, Combination.
- in a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.
- in a locked vault or VTR outside an LA, EA, PA, or MAA that must be under IDS protection. The PF must respond within five minutes of alarm annunciation.

**e) Describe the difference between the storage of Top Secret and Secret matter.**

Secret matter must be stored in a manner authorized for Top Secret matter or

- in a locked vault (requirements for vaults are included in DOE M 470.4-2, Physical Protection) or in a locked GSA-approved security container within an LA or higher.
- in a locked VTR (requirements for VTRs are included in DOE M 470.4-2, Physical Protection) within an LA, EA, PA, or MAA equipped with IDS protection. The PF must respond within 30 minutes of alarm annunciation.
- when located outside an LA, the locked vault or VTR must be under IDS protection. The PF must respond within 15 minutes of alarm annunciation.
- in locked, steel filing cabinets that do not meet GSA requirements (containers purchased and approved for use before July 15, 1994, may continue to be used until October 1, 2012) and are equipped with three-position, dial-type, changeable combination locks. The cabinet must be in a locked area or building within the minimum of an LA, EA, PA, or MAA.

In addition, one of the following supplemental controls is required:

- IDS protection that provides for response from PF personnel within 30 minutes of alarm annunciation when the area is unattended;
- inspection every four hours by PF, or by cleared duty personnel when unattended.

**f) Describe the differences between the storage of Secret and Confidential matter.**

Confidential matter must be stored in the same manner prescribed for Top Secret or Secret matter, but the supplemental controls are not required.

**g) Describe the responsibilities in the event that a repository or location containing classified matter is found unattended.**

Incidents of security concern are actions, inactions, or events that have occurred at a site that

- pose threats to national security interests and/or critical DOE assets
- create potentially serious or dangerous security situations
- potentially endanger the health and safety of the workforce or public (excluding safety-related items)
- degrade the effectiveness of the S&S program
- adversely impact the ability of organizations to protect DOE S&S interests

Incidents of security concern must be categorized in accordance with their potential to cause serious damage or place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, PF, information security, personnel security, and nuclear MC&A. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

*Reporting Requirements*

The 24-Hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens) must be sent to the DOE HQ OC using DOE Form (F) 471.1, Security Incident Notification Report, in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria:

- Within one hour following categorization for security incidents determined to be IMI-1, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

- Within eight hours following categorization of security incidents determined to be IMI-2/IMI-3, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

*Data Collection*

If a repository/location containing classified information is found unattended, perform the following tasks:

- Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
- Conduct interviews to obtain additional information regarding the incident.
- Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, and readouts from monitoring equipment, etc.)
- Ensure physical evidence is protected and controlled and a chain-of-custody is maintained.

*Incident Reconstruction*

Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence. Develop a chronological sequence of events that describes the actions preceding and following the incident. Identify persons associated with the incident.

*Incident Analysis and Evaluation*

This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must

- analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately
- collect additional data and reconstruct the incident if more information is required
- identify any collateral impact with other programs or security interests

**h) Describe responsibilities in response to an intrusion detection alarm on a repository or location containing classified matter.**

Top Secret matter must be stored

- in a locked, GSA-approved security container with one of the following supplemental controls: (1) under IDS protection and by PF personnel responding within 15 minutes of alarm annunciation, or (2) with inspections by PF personnel occurring no less frequently than every two hours. If the container is located in an LA, EA, PA, or MAA, the GSA-approved security container must have a lock meeting federal specification FF-L-2740A, Locks, Combination.
- in a locked vault or VTR within an LA, EA, PA, or MAA. The vault or VTR must be equipped with intrusion detection equipment, and PF personnel must respond within 15 minutes of alarm annunciation.

- in a locked vault or VTR outside an LA, EA, PA, or MAA that must be under IDS protection. The PF must respond within five minutes of alarm annunciation.

Secret matter must be stored

- in a locked VTR within an LA, EA, PA, or MAA equipped with IDS protection. The PF must respond within 30 minutes of alarm annunciation.
- so that when located outside an LA, the locked vault or VTR is under IDS protection. The PF must respond within 15 minutes of alarm annunciation.

Complete nuclear weapon configurations, nuclear test and trainer devices, and nuclear-explosive-like assemblies without nuclear material must be stored in a vault or VTR located, at a minimum, within an LA. PF personnel must respond within 15 minutes of alarm annunciation.

**i) Describe the procedures for receiving and transmitting classified matter.**

Classified matter must be transmitted only in the performance of official or contractual duties. If the transmission is not required by the specific terms of the contract or required for performance of the contract, contractors must obtain written authorization from the DOE cognizant security authority before transmitting classified matter outside the facility. Before transmitting classified matter, the sender must ensure that the recipient has the appropriate access authorization or clearance, has any required programmatic or special access approval, meets the "need to know" criteria, and has an approved classified address.

*Receiving*

When classified matter is received at a facility, the following controls must apply:

- Classified matter must be delivered to personnel designated to receive it at a control station with the inner envelope unopened. Procedures must be established to ensure that when classified matter is not received directly by the designated control station (regardless of the type of mail system), the inner container remains unopened. Though the inner envelope must not be opened before delivery at the control station, the outer envelope may be opened if local procedures permit.
- The package must be examined for evidence of tampering and the classified contents checked against the receipt (if provided). Evidence of tampering must be maintained and reported promptly to the cognizant security authority. If the matter was received through the U.S. Postal Service, the appropriate U.S. Postal Inspector must also be notified promptly. Discrepancies in the contents of a package must be reported immediately to the sender. If the shipment is in order and includes a receipt, the receipt must be signed and returned to the sender. A copy of the receipt must be maintained with the control station records.

*Packaging*

Classified matter to be transmitted outside a facility must be double-wrapped (enclosed in opaque inner and outer containers) except as specified below.

*Envelopes and Similar Wrappers*

When envelopes are used for packaging, the classified information must be protected from direct contact with the inner envelope. This is accomplished by having a cover sheet on the

front of the document and a sheet of paper or cover sheet to protect the back of the document if the document has information on the back page. Additionally, the following requirements apply:

- The overall classification level of the contents must be marked on the top and bottom of the front and back of the inner container.
- The category (if RD or FRD) and caveats (if applicable) or special markings must be placed on the front of the inner container.
- The inner container must be sealed. The sender's classified address should appear in the upper left corner and the recipient's classified address should be centered on the front of the container.
- The outer envelope or container must be sealed and marked with the recipient's and sender's classified mailing addresses (mailing, shipping, or overnight, as appropriate).
- The outer envelope must not carry markings indicating the contents are classified.

When opaque containers (i.e., envelopes) are temporarily unavailable, appropriate measures must be taken to ensure that the contents of the document cannot be seen through the inner container and that the security markings on the inner container cannot be seen through the outer container. All the seams of an envelope or wrapper must be sealed with tamper-resistant tape (e.g., fiber tape) or be constructed in a manner designed to provide tamper indication (e.g., tamper-evidence security bags) to prevent undetected access to the contents while in transit. Note: Outer containers must meet U.S. Postal Service regulations for registered packages.

*Other Containers*

If the item is of a size, bulk, weight, or nature that precludes the use of envelopes for packaging, other containers of sufficient strength and durability must be used to protect the item while in transit. The following requirements apply:

- To prevent items from breaking out and to facilitate the detection of tampering, tamper-resistant material (such as seals, puncture resistant material, or wire mesh) must be used for packaging.
- As long as the item is enclosed in a double container, the matter may be wrapped or boxed in paper, wood, metal, or a combination thereof.
- The inner package must be addressed to a classified address, return-addressed to a classified address, and marked with the overall classification level and category (if RD or FRD) of the contents and any appropriate caveats.
- The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed, with no markings to indicate the contents are classified.
- If specialized shipping containers, including closed cargo transporters, are used for transmitting classified matter, the shipping container may be considered the outer container. The following stipulations apply:
    - The address may be omitted from the inner and outer container for shipments in full truckload lots when such an exception is contained in the provisions of the contract.
    - Under no circumstances will the outer container or the shipping document attached to the outer container reflect the classification of the contents or the fact that the contents are classified.

*Equipment Components*

If the classified matter is an internal component of a packaged item of equipment with an outside shell or body that is unclassified and that completely shields the classified internal component from view, the shell or body may be considered the inner container. The shell or body must be marked with the classification level and category (if RD or FRD) of the equipment, but the address and return address may be omitted. The outer container must be addressed to a classified address, return-addressed to a classified mailing address, and sealed with no markings or notations to indicate the contents are classified.

If the classified matter is an inaccessible internal component of a bulky item of equipment that cannot be reasonably packaged, such as a missile, no inner container is required and the outside shell or body may be considered the outer container if it is unclassified. If the shell or body is classified, the matter must be draped with an opaque covering that will conceal all classified features. The covering must be capable of being secured to prevent inadvertent exposure of the item.

*Locked Briefcases*

If a locked briefcase is used to hand-carry classified matter of any level, the briefcase may serve as the outer container. The requirement that an individual carrying a briefcase with classified matter outside a security area must possess a DOE Form (F) 5635.13, Authority to Hand-Carry Classified Matter, is no longer in effect. (If local procedures require use of hand-carry cards, sites may develop local hand-carry forms.) The following requirements apply:

- The inner container must be sealed, addressed with the sender's and recipient's classified addresses, and marked with the overall classification level and category (if RD or FRD) of the contents and caveats (if applicable).
- The briefcase (outer container) must indicate the return classified address and must contain no markings to indicate the contents are classified.
- A briefcase may not serve as the outer container for travel aboard commercial aircraft.

*Offsite Transmittal and Receipts*

DOE F 5635.3, Classified Document Receipt, or a receipt comparable in content must be used to transmit accountable and classified matter outside of facilities. Receipts must identify the classified contents and the names and addresses of both the sending and receiving facilities. Receipts must not contain classified information. The receipt must be placed inside the inner container. If not practical, the receipt may be sent to the recipient with the required advance notification of shipment or may be hand-carried. When classified matter is transmitted by courier, DOE F 5635.3, or a receipt comparable in content, must be used.

*Receipt Information*

The receipt must be prepared in triplicate and remain unclassified when completed. Two copies of the receipt must be placed in the inner container with the matter (except as noted above) and sent to the intended recipient. The third copy must be maintained by the sender until the original is signed and returned. The receipt must contain the following information:

- Full names of the sender and the recipient
- Classified address of the sender

- Classified address of the recipient
- Description of the classified matter (e.g., title or other means)
- Date of the matter
- Classification of the matter
- Unique identification number, if accountable

*Multiple Items*

If all items are going to one recipient, one receipt may be used for multiple items. Regardless of the number of items being transmitted, one receipt should be completed for each recipient. Check any special mailing instructions included in the classified mailing address in the Safeguards and Security Information Management System.

*Exceptions*

Receipts are not required for non-accountable classified matter under the following conditions:

- For transmittal of matter within a facility
- For transmittal of confidential matter

*Facsimile Transmission*

Individuals transmitting classified information through facsimile systems must confirm receipt (verbally or in writing) with the intended recipient as follows:

- A receipt, such as DOE F 5635.3, may be completed and transmitted with the classified message by means of facsimile systems. Upon receiving the facsimile, the recipient would complete the receipt and return it also by facsimile.
- An acceptable alternative would be to contact the intended recipient and notify him/her that a classified message is being transmitted by facsimile. Upon receipt, the recipient must telephone the sender to verify the complete transmission was received. This verbal communication must be documented and retained and will suffice for all other written forms of receipt.

*Classified Addresses*

Requirements for classified addresses are as follows:

- Classified matter must be addressed only to approved classified addresses for mailing, shipping, or overnight delivery, contingent upon the appropriate method of transmission.
- Classified addresses must be verified through the Safeguards and Security Information Management System (SSIMS), except as otherwise noted, for
  - companies where there is a DOE contractual interest;
  - OGA contractors where there is no contractual agreement with DOE, and the interest includes RD, FRD, or weapons data information;
  - companies where there is no DOE contractual agreement for NSI. (Note: Defense Security Service [DSS] may also be used for verifying classified addresses approved for NSI.)
- Hardcopies of classified addresses obtained through SSIMS or DSS are only valid for 30 calendar days.

- A Classified Mail Channel may be established in SSIMS for an OGA contractor organization where DOE or NNSA does not have a contractual interest. To establish an address for the Classified Mail Channel, a Statement of Security Assurance, or a form comparable in content, must be completed and signed by the cognizant security authority and authorizing Government official for the OGA contractor. Also see DOE M 470.4-1, Safeguards and Security Program Planning and Management, Facility Clearance Program. Once the form is completed, the information must be entered into SSIMS. This process may only be used when the contractor facility has been approved by another Government agency and registered in SSIMS, and must not be used as a basis for granting facility security approvals.
- Alternative methods for verifying classified addresses must be approved by the Office of Security.
- Office code letters, numbers, or phrases must be used in an attention line for internal routing. A recipient's name may be used in addition to office code letters, numbers, or phrases.
- When classified matter must be sent to an individual or consultant operating at a cleared facility other than his or her own, or when classified matter must be sent to any approved facility at which only one cleared employee is assigned, the outer container must specify the following: TO BE OPENED BY ADDRESSEE ONLY. Postmaster—Do Not Forward. If Undeliverable to Addressee, Return to Sender.
- Mail addressed as indicated above must be accepted only by the addressee or by an agent the addressee has authorized in writing to receive such mail. Only personnel who have an appropriate access authorization may be designated as agents for the addressee.

**j) Describe the procedures for packaging classified matter for transmission outside of the facility.**

See element "i," above.

**k) Discuss the procedures for transmitting classified matter outside of the security area.**

See element "i," above.

**l) Describe the different ways of transmitting classified matter.**

See element "i," above.

**m) Discuss the guidelines used for the reproduction of classified documents.**

*General Guidelines*

The general guidelines for the reproduction of classified documents are listed below:

- Classified documents may be reproduced without originator approval except when they contain markings that limit reproduction without specific written originator approval.
- Accountable classified removable electronic media (ACREM) may be reproduced when any of the data that resides on a piece of ACREM is to be copied onto a piece of media that has already been placed into the formal accountability system, provided there are no other limitations. Permission is required from the DOE cognizant security authority before copying any of the data that resides on a piece of ACREM onto a piece of media that has not already been placed into the formal accountability system.

- If a classified document needs to be copied immediately, and the document contains a caveat limiting reproduction without originator approval, the following procedure must be used:
  - Gain originator approval by telephone.
  - Make the minimum number of copies required. Following normal procedures, destroy unneeded copies immediately after the emergency use.
  - Follow up by obtaining permission in writing as soon as possible.
- The cognizant security authority must establish local controls for the reproduction of classified documents. Reproduction of classified documents must be limited to the minimum number of copies consistent with operational requirements and any further reproduction limitations shown on the document. Local procedures should address the issue of controlling the number of copies of classified documents. To restrict reproduction of a classified document, consider one of the following techniques:
  - For intelligence documents only, the Director of Central Intelligence ORCON caveat marking may be used to restrict reproduction to that allowed by the originator.
  - Originators of non-intelligence documents who wish to prevent unlimited copying of a classified document may use the markings specified in DOE M470.4-4 or others similar in content.
- Reproduction must be accomplished by authorized persons who know the procedures for classified reproduction and only in the performance of official or contractual duties.
- Reproduced copies are subject to the same protection and control requirements as the originals.
- Reproduction restrictions must not constrain the reproduction of documents to facilitate review for declassification. However, after such reviews, reproduced documents remaining classified must be destroyed in accordance with requirements.

*Equipment*

Classified documents must be reproduced on equipment specifically approved and designated for this purpose to ensure minimal risk of unauthorized disclosure. To the greatest extent possible, these machines must be located within LA, PAs, or EAs. Additional requirements are listed below:

- Access to Machines. Classified documents must be reproduced under appropriate security conditions to preclude unauthorized access to classified information. Classified copying must not be performed in the presence of individuals lacking the proper access authorizations.
- Notices. Notices regarding the restrictions and requirements of reproducing classified documents must be posted conspicuously next to the equipment.
- Clearing. Ensure that no classified waste is trapped or left in the equipment and clear all possible residual classified images after classified reproduction. Local procedures and copier design will dictate how the copier should be sanitized.
- Approval. Ensure that all machines to be used for reproducing classified documents are approved in accordance with local procedures and cyber security policy. At a minimum, ensure that
  - classified copy machines do not have modems or the ability to be connected to an external modem;

- contracts for new digital copy machines specify that memory chips will not be removed without permission, and that any remote diagnostics capabilities will be disabled.

In areas where routine Technical Surveillance Countermeasures (TSCM) services occur, reproduction machines must be examined by a certified TSCM team prior to introduction into the area.

**n) Describe the proper way to dispose of classified matter.**

*Destruction of Classified Matter*

Procedures must be established for the ongoing review of classified holdings to reduce volume to the minimum necessary. Multiple copies, obsolete matter, and classified waste must be destroyed as soon as practical. Classified matter must be destroyed in accordance with records disposition schedules.

If under a court order prohibiting destruction, special destruction procedures may be required. Under such circumstances, all destruction activities must be conducted in accordance with guidance provided by the DOE Office of General Counsel and the appropriate records management organization.

Classified matter must be destroyed beyond recognition to preclude reconstruction. Destruction can be accomplished by burning, shredding, pulping, melting, mutilating, pulverizing, or by chemical decomposition. The following additional requirements must be satisfied when classified matter is destroyed:

- The DOE cognizant security authority must approve the use of public destruction facilities or any other alternative procedures (e.g., burying or disassembly).
- If classified matter cannot be destroyed onsite, it must be destroyed at a public destruction facility by a cleared individual on the same day it is removed from the site. A record of dispatch is not required unless custody of the matter is released to another cleared contractor or OGA.
- Ash residue produced by burning must be examined and reduced by physical disturbance to ensure that the matter is completely destroyed and no unburned matter remains.
- Classified microforms must be destroyed by burning, chemical decomposition, disintegration, or other methods approved by the cognizant security authority.
- Classified automated information systems media must be destroyed by pulverizing, smelting, incinerating, disintegrating, or using other appropriate methods.
- For printing operations, the "regaining" of reproduction plates is not an authorized method of destruction. Impressions of classified information must be destroyed at the end of the run by cleaning the rollers and other parts of the presses to remove the classified information.
- Some destruction methods may pose environmental hazards creating environmental concerns. In addition to obtaining DOE cognizant security authority approval to destroy classified matter by such methods, site personnel must determine whether approval is also required by federal and state environmental protection agencies.
- For burial of classified matter, the primary concern is the likelihood of retrieval. Burial should be reserved for non-paper matter only, if possible. When contemplating burial as a destruction option, the cognizant security authority must consider the following:

- The location within the burial grounds for classified matter
- Access controls
- The difficulty of retrieval through some type of "entombment" process (e.g., encasement in concrete)
- Health and safety measures for contaminated classified matter

*Equipment*

Classified matter must be destroyed by equipment that has been approved by the cognizant security authority. The residue output must be inspected each time destruction is effected to ensure that established requirements have been met. Procedures must be established to ensure compliance with the manufacturer's instructions, as appropriate, for operating destruction equipment and to ensure continuing effectiveness. Additional requirements are listed below:

- Shredders. Crosscut shredders used for the destruction of classified paper matter and non-paper products, excluding microfilm, must produce residue with a particle size not exceeding 1 mm in width by 5 mm in length. Crosscut shredders purchased prior to December 31, 2003, that produce residue with particle sizes not exceeding 1/32 of an inch in width by 1/2 inch in length may continue to be used for the destruction of classified paper matter and non-paper products, excluding microfilm. However, these shredders must not be used once they cannot be repaired or restored to cut residue within the 1/32 inch width by 1/2 inch maximum particle dimensions.
- Pulping equipment must be equipped with security screens with perforations of 1/4 inch or smaller.
- Pulverizing equipment must be outfitted with security screens that meet the following specifications:
  - Hammer mill perforations must not exceed 3/16 inch in diameter.
  - Chopper and hybridized disintegrator perforations must not exceed 3/32 inch in diameter.

*Witnesses*

The destruction of classified matter must be accomplished by individuals who have appropriate access authorization for the classification level of the matter to be destroyed.

The destruction of non-accountable classified matter may be accomplished by one individual; no witness is required.

The destruction of accountable classified matter must be witnessed by an appropriately cleared individual other than the person destroying the matter. Locations with only one employee with appropriate access authorization must contact their cognizant security authority for guidance on destruction.

*Classified Waste*

Classified waste must be destroyed by approved methods as soon as practical. Receptacles used to accumulate classified waste must be clearly marked to indicate their purpose. Pending destruction, classified waste and receptacles must be protected as required for the level and category of classified matter involved. Non-accountable classified matter (i.e., any matter classified as secret or confidential that is not entered into an accountability system) may be destroyed as classified scrap or waste. Examples of classified scrap or waste include

typewriter, teletype, and dot matrix ribbons; notes, drafts, and working papers; carbon paper copies; X rays; imperfect copies of master documents; and any matter in excess of operational needs.

**o) Describe the accountability records that must be maintained for accountable classified matter.**

Destruction of accountable classified matter must be documented on DOE F 5635.9, Record of Destruction, or a form similar in content, which must be signed by both the individual destroying the matter and the witness. An audit trail must be maintained until destruction. Destruction records must be maintained in accordance with the DOE records schedule.

**p) Describe the proper way to mark a classified document.**

*General Requirements*

Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD). Documents must be marked in accordance with directives in place at the time of origin or later, or in accordance with current directives. If there is a question about the classification level or category of a document, the document must be reviewed by a derivative classifier and re-marked (if necessary) to clearly indicate the level and category and to ensure proper protection. When possible, avoid returning documents because of improper markings. Instead, contact the sender and attempt to resolve any marking issues.

Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings, including declassification on a date or event, classification authority, or classifier's name, should be reviewed by a derivative classifier to ensure the classification level and category are still correct and then re-marked to bring them into conformance with current marking requirements. This must be done if the document is active or is to be transmitted outside of the organization for other than official archiving purposes. Documents created before April 1, 1996, need only contain classification level and category (if RD or FRD) to ensure proper protection.

Before using or distributing a document marked with the following obsolete markings, a derivative classifier or declassifier must determine the classification status and mark the document accordingly. DOE M 475.1-1A, Identifying Classified Information, provides requirements for reviewing and marking these documents. Pending review, documents must be handled and protected as Confidential/National Security Information (C/NSI).

- Restricted. This is an obsolete U.S. classification marking used before December 15, 1953, that identifies a security level less sensitive than Confidential. This marking is still used by some foreign governments and international organizations.
- Official Use Only (OUO). The Atomic Energy Commission used this term between July 18, 1949, and October 22, 1951, as an equivalent to the term Restricted. This marking is now used to identify unclassified information that may be exempt from disclosure under the Freedom of Information Act (FOIA).

*Markings*

The following elements are common to all classified documents: classification level, classification category (if RD or FRD), caveats and/or special markings (if required), classifier information, originator identification, classification of titles or subjects, unique identification numbers (if in accountability), and portion marking (if NSI). The DOE Marking Handbook provides guidance and examples for marking classified documents. The originator is responsible for ensuring that each classified document is marked correctly.

*Unique Identification Numbers*

Classified matter required to be in accountability must have a unique identification number. To ensure control and accountability of this matter, the unique identification number must be placed on the first page of paper documents and on the top or front of non-paper documents. The first page of a document is the first sheet of paper (i.e., the cover page, title page, or first page of text).

*Originating Organization and Date*

The name of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents. The first page of a document is the first sheet of paper, whether that is the cover page, title page, or first page of text. Classified documents being taken offsite must be marked on the first page to show the mailing address of the organization responsible for preparing the document. The mailing address should consist of a street address or post office box, city, state, and zip code.

*Classification Level*

The three classification levels, in descending order of sensitivity and potential damage to the national security, are Top Secret, Secret, and Confidential. Requirements for marking classified documents and materials are listed below:

- The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text.
- Each interior page of a classified document must be marked top and bottom with the highest classification level (or marked unclassified if applicable) of that page or the overall classification of the document.
- Classification markings must be clearly distinguishable from the document text.
- Classified material must have the classification level stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.
- Blank interior pages of a classified document need not be marked with the classification level or category or the notice "This page intentionally left blank."

*Classification Categories*

The three classification categories are RD, FRD, and NSI. Classified documents containing only NSI need not be marked with the NSI category marking. If the document is RD or FRD, the appropriate admonishment information must be marked on the first page of the document, whether that be the cover page, title page, or first page of text, and should appear in the lower left corner, as follows:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

FORMERLY RESTRICTED DATA
Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination per Section 144.b, Atomic Energy Act, 1954.

Each interior page of a document containing RD or FRD must be marked top and bottom with the appropriate level and category of information on that page. If this is not feasible, the overall level and category of the document (if RD or FRD) may be applied to every page. For interior pages, the symbols RD and FRD may be used. These markings must be clearly distinguishable from the document text.

Classified material (if RD or FRD) must have the classification category stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.

RD or FRD documents generated prior to July 9, 1998, will not be required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the office of origin or holder for other than archiving purposes.

*Mixed Levels and Categories*

DOE policy states that matter must be classified and marked at the highest level and category of the information contained in it. When classified matter contains a mix of information at various levels and categories that cause the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow access by an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized to access if the document was only marked at the highest overall classification level and category. For example, a document that contains Confidential RD (C/RD) and Secret NSI (S/NSI) information would be required to be marked at the highest level and category, which is Secret RD (S/RD) in this case, even though none of the information in the document is actually S/RD. However, this may not be interpreted to authorize any individual to gain access to information which exceeds their access authorization, formal access approvals, and "need to know." If a matrix is used, the following marking matrix, or one similar in content, will be used in addition to other required markings, and must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking. The derivative classifier's name and title are required only when a document is reviewed after the initial classification determination has been made and the mixed level and category marking is applied.

This document contains:
Restricted Data at the (e.g., Confidential) level.
Formerly Restricted Data at the (e.g., Secret) level.
National Security Information at the (e.g., Secret) level.
Classified by: Name and Title.

*Components*

When components of a document are to be used separately, each major component must be marked as a separate document. Components include annexes or appendices, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are Unclassified."). When this method of marking is used, no further markings are required on the unclassified component.

*Unclassified Matter*

Unclassified matter need not be marked unless it is essential to convey one of the following conditions:

- The matter has been reviewed for classification and does not contain classified information.
- The matter has been properly declassified.

If unclassified matter is to be marked, the Unclassified marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.

Unclassified information must not be marked in a manner that would be confused with markings specified for classified information (e.g., Confidential). If the unclassified matter carries a control marking (i.e., OUO, Unclassified Controlled Nuclear Information [UCNI], or Export Controlled Information [ECI]), the information must retain its control marking; it should not be re-marked unclassified.

*Portions*

For NSI documents, each section, part, paragraph, graphic, figure, or similar portion of any such document dated after April 1, 1997, must be marked to show the classification level, or be identified as unclassified controlled information (e.g., UCNI, OUO) or as unclassified (U). Classification levels of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.

Page changes to NSI documents dated after April 1, 1997, must be portion marked. Additionally, any NSI document that becomes active (i.e., when sent outside the office of origin or holder other than for archival storage, or when removed from storage) must be portion marked with the appropriate classification level, unclassified controlled symbol (e.g., UCNI, OUO, etc.), or unclassified. If any NSI document dated before April 1, 1997, is sent outside the office of origin or holder for other than archiving purposes, the entire document must be portion marked.

Documents containing RD or FRD are not required to be portion marked. However, in cases where portion markings are used, classification levels and categories (if RD or FRD) of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers,

immediately before the beginning of the portion. Each section, part, paragraph graphic, figure, or similar portion of any such document must be accurately marked to show the following:

- The classification level and category (SRD or S/RD, CFRD or C/FRD, S, TS, etc.)
- That it is unclassified controlled information (e.g., UCNI, OUO)
- That it is unclassified (U)

Portion markings must include any applicable caveats.

Portions of U.S. documents containing Foreign Government Information (FGI) must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-Confidential). FGI must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.

Classified documents generated by foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the level the foreign government specified.

Portions of U.S. documents containing North Atlantic Treaty Organization (NATO) information must indicate NATO or COSMIC (NATO Top Secret documents), including the appropriate classification level (e.g., NATO-S or COSMIC-TS).

*Compilations*

In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification level and category (if RD or FRD) assigned to the document must be conspicuously marked or stamped at the top and bottom of each page, on the back of the last page of the document, and on the front cover, if any. A document classified for this reason is not required to be portion marked, but must contain the following statement on the first page: "This document has been classified under the compilation concept and shall not be used as the source for a derivative classification decision." The reason for classifying the information as a compilation also must be stated at an appropriate location near the beginning of the document.

*Subjects and Titles*

Except for extraordinary circumstances, unclassified subject descriptors and titles must be used for classified documents because they are used on mail logs, document receipts, and other tracking or accountability records, most of which are entered into unclassified databases. Titles of classified documents must be marked even if the document is not portion marked.

If subjects or titles are classified, they must be marked with the appropriate classification level, category (if RD or FRD), and any applicable caveats. If titles are not classified, they must be marked as unclassified or with the appropriate unclassified controlled marking (e.g., OUO).

The classification or control symbols (e.g., U, OUO, UCNI, C/RD, S/FRD) must be placed immediately after the title or subject.

When classified documents with unmarked titles and/or subjects become active (i.e., sent outside the office of origin or holder, or removed from storage), the titles and/or subjects must be reviewed by a derivative classifier and marked appropriately.

If a caveat (e.g., originator controlled [ORCON]) applies to the title or subject, it must be added to the title marking. A Secret NSI/ORCON title must be shown as S/ORCON.

*Authorized Markings for Portions, Subjects, and Titles*

The following are examples of the markings authorized for use with subjects and titles and when portion marking:

Unclassified: (U)
Official Use Only: (OUO)
Unclassified Controlled Nuclear Information: (UCNI)
Confidential National Security Information: (C)
Confidential Formerly Restricted Data: (C/FRD) or (CFRD)
Confidential Restricted Data: (C/RD) or (CRD)
Secret National Security Information: (S)
Secret Formerly Restricted Data: (S/FRD) or (SFRD)
Secret Restricted Data: (S/RD) or (SRD)
Top Secret National Security Information: (TS)
Top Secret Restricted Data: (TS/RD) or (TSRD)
Top Secret Formerly Restricted Data: (TS/FRD) or (TSFRD)

*Classifier Markings*

Classifier marking requirements can be found in DOE M 475.1-1A, Identifying Classified Information.

*Director of Central Intelligence Information*

The following markings, unless indicated otherwise, are authorized only for use for intelligence information:

- No Foreign Dissemination (NOFORN). This marking indicates the information contained in the document may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. This marking may be used for intelligence information and Naval Nuclear Propulsion Information (NNPI) only.
- ORCON. This marking indicates the document bearing the marking is controlled by the originator. Reproduction of, extraction of information from, or redistribution of such a document requires the permission of the originator. This marking must be used only on classified documents containing intelligence information that clearly identifies, or would reasonably permit the identification of, intelligence sources or methods. It must not be used when access to the information can be reasonably protected by its classification markings or any other control markings. Without advanced permission from the originator, the dissemination of ORCON beyond the DOE Headquarters intelligence components and the formally designated field intelligence elements is limited. As a condition for receipt of ORCON by a non-intelligence component, written assurance that the recipient will observe the provisions of the Director of Central Intelligence Directive must be provided to the Office of Intelligence.

- Proprietary Information (PROPIN). This marking indicates the information contained in the document must not be released outside the Federal Government in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information without the permission of the originator of the intelligence information and provider of the proprietary information. This precludes dissemination to contractors, irrespective of their status within the Government, without the above consent.
- Authorized for Release to Country (REL TO). This marking applies to intelligence information the originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to specified foreign countries or international organizations. The name of country or countries authorized access to the document must be included after the caveat (e.g., REL TO Canada, United Kingdom). The name of the country may be spelled out or abbreviated, but must be identifiable.

*Obsolete Markings*

The following markings are no longer used, but remain applicable on the documents that bear these markings until such time as the documents are re-reviewed and re-marked:

- No Dissemination to Contractors (NOCONTRACT)
- Warning Notice Intelligence Sources and Methods (WNINTEL)

Note: Existing instances of these markings remain valid until the documents containing them are re-reviewed and re-marked for classification purposes, or until they become declassified.

*Remarking Upgraded, Downgraded, and Declassified Matter*

When an official upgrade, downgrade, or declassification notice is received, the initial classification markings must be stricken and replaced with the new classification markings. The authority for and date of the upgrading, downgrading, or declassification notice must be entered on the first page of the document. The originator or document custodian must notify all known holders of the document.

Upgrading. A derivative classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of an upgrade notice from the proper authority. The originator or document custodian must notify all known holders with the proper access authorization when a document has been upgraded. Upon receipt of the authorization to upgrade a classified document, the first page of the document must be marked to show the date the classified document was upgraded and authority for upgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

Downgrading. A derivative declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of a downgrade notice from the proper authority. When the authorization to downgrade a classified document is received, the first page of the document must be marked to show the date the classified document was downgraded and authority for downgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

**q) Describe the procedures for handling classified matter through the process of a contract termination or facility closeout.**

When a contract is completed, the contractor usually destroys or returns all classified matter unless it provides a benefit to DOE for the contractor to retain the classified matter. Upon completion or termination of a contract, the contractor must submit to the contracting officer either a certificate of non-possession or a certificate of possession (of classified matter). The contracting officer must then transmit the certificate to the DOE cognizant security authority.

*Certificates of Non-Possession*

Upon return or destruction of all classified matter pertaining to a contract, the contractor must submit a certificate of non-possession to the cognizant security authority. The certificate must include the contract number and a statement that all classified matter has been returned or destroyed.

*Certificates of Possession*

Requests to retain classified matter must indicate the benefit to DOE and the intended use of the information. Certificates must specifically identify classified matter by subject, type or form, and quantity. If the classified matter will aid the contractor in performing another active Government contract and the matter is being transferred to the active contract, the contractor must provide the DOE cognizant security authority or the OGA holding the contract a copy of the retention notification. If the contractor is not notified to the contrary, the matter may be transferred and will fall under the jurisdiction of the gaining (i.e., active) contract. When a certificate of possession is submitted, the contractor may maintain the classified matter for 24 months unless notified to the contrary by the DOE cognizant security authority or OGA.

*Termination of Facility Clearance*

Notwithstanding the provisions for retention outlined above, if a facility clearance is terminated for any reason, classified matter in the facility's possession must be returned to DOE or disposed of in accordance with instructions from the cognizant security authority. A certificate of non-possession must be completed as part of the clearance termination process. For prime contracts, DOE is the cognizant security authority. To accomplish the termination requirements, the cognizant security authority must ensure the following steps are accomplished:

- Determine whether a moratorium or ongoing litigation restricts actions.
- Acquire all classified matter not authorized for destruction.
- Conduct a 100 percent inventory of all accountable matter, taking appropriate action if any matter is missing.
- Check to ensure that all matter has been returned, if applicable.
- Destroy all copies, except record copies, of all classified documents.
- Send all remaining classified matter to the site specified by the responsible contracting officer and cognizant security authority.

Once the matter is destroyed or transferred, the cognizant security authority must complete the facility termination procedures (see DOE M 470.4-1, Safeguards and Security Program Planning and Management).

**r) Describe the process used to report, assign, and resolve the loss of classified matter.**

Incidents of security concern are actions, inactions, or events that have occurred at a site that

- pose threats to national security interests and/or critical DOE assets
- create potentially serious or dangerous security situations
- potentially endanger the health and safety of the workforce or public (excluding safety-related items)
- degrade the effectiveness of the S&S program
- adversely impact the ability of organizations to protect DOE S&S interests

Incidents of security concern must be categorized in accordance with their potential to cause serious damage or to place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an impact measurement index (IMI) number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, PF, information security, personnel security, and nuclear MC&A. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

*Reporting Requirements*

The 24-Hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens) must be sent to the DOE HQ OC using DOE F 471.1, Security Incident Notification Report, in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria:

- Within one hour following categorization for security incidents determined to be IMI-1, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.
- Within eight hours following categorization of security incidents determined to be IMI-2/IMI-3, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within eight hours of any security incidents

that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1, and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the OCI/ODNCI must be notified.

Numbering Incidents and Changing Categories. When the initial incident notification report (i.e., DOE F 471.1) is transmitted, it must include a local incident tracking number. All subsequent reports pertaining to a security incident (e.g., inquiry and other related activities) must be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 (or form similar in content) to the Office of Security.

Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the SCI Program, the SAP, the TSCM Program, the CI Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report must be transmitted to the Office of Security for entry into the Incident Tracking and Analysis Capability database.

Inquiries are considered closed under the following conditions:

- IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided.
- IMI-3 incidents are considered closed upon completion of DOE F 5639.3, Report of Security Incident/Infraction, and transmission of the completed DOE F 5639.3 to the Office of Security. The completion of the section on assignment and acceptance of security infractions (Part II, DOE F 5639.3) must be completed as required in local procedures.
- IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 in accordance with associated local procedures.

A sanitized (unclassified) copy of the DOE F 5639.3 must be provided to the responsible personnel security office for placement in the appropriate personnel security file.

*Final Inquiry Reports*

Inquiry officials must forward final inquiry reports in accordance with local procedures to line management for action and to the Office of Security.

*Inquiry Officials*

Requirements for inquiry officials are as follows:

- Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.

- Inquiry officials may be either federal or contractor employees, but must have previous investigative experience or Department inquiry training, and must be knowledgeable of appropriate laws, Executive orders, Departmental directives, and/or regulatory requirements.
- Inquiry officials are not authorized to detain individuals for interviews or to obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.
- Inquiry officials must be appointed in writing by the DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.
- Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).
- When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

*Conduct of Inquiries*

If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry:

- If the sites/facilities fall under the purview of a single DOE cognizant security authority, that DOE cognizant security authority must assign responsibility to a lead organization.
- If the sites/facilities fall under the purview of multiple DOE cognizant security authorities, those DOE cognizant security authorities must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report:

- Data Collection.
  - Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
  - Conduct interviews to obtain additional information regarding the incident.
  - Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, readouts from monitoring equipment, etc.)
  - Ensure physical evidence is protected and controlled and a chain of custody is maintained.
- Incident Reconstruction.
  - Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
  - Develop a chronological sequence of events that describes the actions preceding and following the incident.
  - Identify persons associated with the incident.

- Incident Analysis and Evaluation.
  This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must perform the following tasks:
  - Analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately.
  - Collect additional data and reconstruct the incident if more information is required.
  - Identify any collateral impact with other programs or security interests.

In addition, inquiry officials must perform the following actions:

- Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.
- Ensure a DOE F 5639.2, Reporting Unaccounted for Documents, or a form comparable in content, is completed if classified information or matter is missing.
- Determine which Departmental element has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.
- Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).
- If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.
- When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the DOJ Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.
  - Could the date and identity of the article or articles disclosing the classified information be provided?
  - Could specific statements in the article that are considered classified be identified? Was the data properly classified?
  - Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.
  - Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?
  - Could the extent and official dissemination of the data be determined?
  - Has it been determined that the data has not been officially released in the past?

- Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?
- Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?
- Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.
- Has it been determined that declassification had not been accomplished prior to the publication or release of the data?
- Will disclosure of the classified data have an adverse impact on the national defense?

**27. Safeguards and security personnel acting in information security shall demonstrate a familiarity-level knowledge of the program described in DOE O 471.2A, Information Security Program.**

Note: DOE O 471.2A, Information Security Program, has been cancelled. A revised reference has been provided below.

**a) Describe the basic elements of a technical surveillance countermeasures program.**

Information on Technical Surveillance Countermeasures can be found in Section E of DOE M 470.4-4. This is an OUO document and must be requested from the DOE Office of Security and Safety Performance Assurance.

**28. Safeguards and security personnel acting in information security shall demonstrate a familiarity-level knowledge of the program outlined in DOE O 471.2A, Chapter II, Operations Security Program.**

Note: DOE O 471.2A, Chapter II, Operations Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-4, Information Security, DOE M 470.4-7, Safeguards and Security Program References, and DOE M 475.1-1A, Identifying Classified Information.

**a) Differentiate between Critical Program Information, formerly known as Critical and Sensitive Information Lists and Indicators, formerly known as Essential Elements of Friendly Information.**

*Critical Program Information*

Critical program information is information concerning sensitive activities, whether classified or unclassified, that is vitally needed by adversaries or competitors for them to plan and act effectively. (Note: Critical program information was formerly defined as information on what was called the "critical and sensitive information list.")

*Indicators*

Indicators are sources of information that, if exploited by an adversary or competitor, could reveal critical program information. An indicator can be identified by asking the question, "If I were an adversary or competitor, where would I go to obtain critical program information?" (Note: Indicators were formerly called "essential elements of friendly information.")

**b) Discuss the basic principles of the Operations Security process:**

- **Identify critical information**
- **Analyze threat**
- **Assess vulnerabilities**
- **Perform risk analysis**
- **Implement countermeasures**

*Identify Critical Information*

Critical information that must be identified consists of specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries or competitors for them to plan and act effectively to guarantee failure or unacceptable consequences for mission accomplishment.

*Analyze Threat*

Threat analysis is a process in which information about a threat or potential threat is subjected to systematic and thorough examination in order to identify significant facts and derive conclusions.

*Assess Vulnerabilities*

Vulnerability analysis is a systematic evaluation process in which qualitative and/or quantitative techniques are applied to detect vulnerabilities and to arrive at an effectiveness level for an S&S system to protect specific targets from specific adversaries and their acts.

*Perform Risk Analysis*

Risk analysis is an analysis of safeguards and/or security system assets and vulnerabilities to establish an expected loss from certain events.

*Implement Countermeasures*

Countermeasures are activities or capabilities that are designed to negate an adversary's ability to exploit vulnerabilities. Under treaties, countermeasures include the use of devices and/or techniques to protect national security, proprietary information, or other critical information while fulfilling state party treaty obligations.

**c) Discuss the basic principles of the selection of countermeasures.**

Information on technical surveillance countermeasures can be found in Section E of DOE M 470.4-4. This is an OUO document and must be requested from the DOE Office of Security and Safety Performance Assurance.

**d) Describe the methodology used to develop a site-specific threat statement.**

To develop a site-specific threat statement, S&S programs must address site-specific characteristics. Performance assurance programs must be developed, managed, and implemented to ensure that S&S programs and protection program elements protect security interests and

activities. These programs must ensure intensive, frequent performance testing of PF individual and unit tactics with oversight by line management and independent oversight organizations.

A management and planning process to achieve integrated, site-specific protection from unauthorized actions must be implemented. This process must be based on a graded approach that implements the integrated concepts of deterrence, prevention, detection, and response.

**e) Describe the purpose and outcomes of a vulnerability assessment (VA).**

A VA includes gathering data that describe the physical and operational characteristics of an S&S system, assigning values such as delay and detection, and analyzing the results to determine the relative effectiveness in conjunction with the adversary's capabilities as identified in the DBT and the Adversary Capabilities List (ACL).

The VA results must be used to determine the following:

- Protection system effectiveness reporting
- The need for S&S upgrades
- Manning/armament levels for the PF
- Justifications for waivers of and exceptions to S&S policy

**29. Safeguards and security personnel acting in information security shall demonstrate an expert-level knowledge of DOE M 475.1-1A, Identifying Classified Information.**

**a) Discuss the responsibilities and authorities of the heads of field elements, field element and contractor classification officers, responsible reviewers, and field element and contractor employees.**

Heads of program and support offices within DOE, including NNSA, ensure that information, documents, and material are reviewed and processed in accordance with the requirements in DOE M 475.1-1.

Heads of DOE elements, NNSA Deputy Administrators, and managers of field elements

- ensure that the necessary staff is designated to fulfill the requirements contained in DOE M 475.1-1;
- ensure that information, documents, and material are reviewed and processed in accordance with the requirements in DOE M 475.1-1;
- ensure that Headquarters classification representatives, classification officers, and other personnel with classification responsibilities participate in the early planning stages of any new program that may generate classified information, documents, or material;
- ensure that the management of classified information is included as a critical element or item to be evaluated in the performance standards of Headquarters classification representatives, classification officers, original classifiers, and any other individuals whose duties include significant involvement in generating classified information, documents, or material;
- identify/appoint an individual to be responsible for notifying the contracting officer of each procurement falling within the scope of DOE M 475.1-1. If such an individual is not identified or appointed, the person originating the procurement request assumes this responsibility.

Headquarters Classification Representatives

- serve as the points of contact with the Office of Nuclear and National Security Information for their Headquarters elements;
- coordinate the classification and declassification reviews of documents and material for their organizations;
- assist individuals within their organizations in implementing the classification and declassification policies and procedures in DOE M 475.1-1, and refer questions, as necessary, to the Office of Nuclear and National Security Information.

Field Element Classification Officers

- serve as the points of contact with the Office of Nuclear and National Security Information for their field elements;
- administer the field element classification and declassification programs;
- ensure that a classification review is performed prior to the dissemination of each document that may be classified, and that is prepared by a field element employee.

**b) Discuss the policies and objectives of the DOE classification program.**

The Office of Nuclear and National Security Information manages the classification and declassification oversight program that ensures that all DOE organizations, including NNSA, and their contractor and subcontractor organizations that generate classified information and documents or material have implemented and maintain an adequate and effective classification and declassification program.

Classification and declassification programs at various facilities differ in scope and complexity. No single list of areas to be covered in an oversight review is appropriate in all cases. Therefore, the scope of the oversight review must be tailored to ensure that it provides the management and oversight necessary to evaluate the adequacy and effectiveness of each individual classification and declassification program.

**c) Discuss the criteria for classification.**

Classification is determined by the classification guidance. At a minimum, classification guidance identifies elements of information that are classified or unclassified in a specific area. For classified information, the guidance prescribes the classification level and category. For information classified as NSI, the guidance also states a concise reason for classifying the information and prescribes declassification instructions or the category for exemption from automatic declassification for each element of information.

**d) Describe the classification levels, and categories, use of the term unclassified, and mosaic compilation.**

*Levels of Classification*

The following levels of classification, listed in descending order of sensitivity, may be applied to RD, FRD, or NSI:

- Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.

- Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- Confidential. The damage tests for RD/FRD and NSI are different, as noted below:
  - RD/FRD. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - NSI. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.

*Categories of Classified Information*

Categories of classified information are as follows:

- RD is information classified under the Atomic Energy Act that concerns the design, manufacture, or utilization of nuclear weapons; the production of special nuclear material; or the use of SNM in the production of energy. RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.
- FRD is information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.
- NSI is information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

*Unclassified*

The term "Unclassified" is used to identify information that is not classified under a statute or Executive order. Unclassified information is not normally marked as "Unclassified" except to distinguish it from classified information, and then only when such a distinction is required or otherwise serves a useful purpose. The fact that information is unclassified does not mean that it may be released to the public.

*Mosaic Compilation*

Under the FOIA, an agency is required to disclose any information that does not fall within one of the FOIA exemptions. However, some information, while seemingly innocuous or suitable for public release on its own, can be extremely harmful when grouped with other information. To provide protection from public disclosure of information that merits protection because of the context in which it is presented, the courts have sanctioned the use of the "mosaic" or "compilation" theory. The compilation approach is explicitly recognized in Executive Order 12958, which sets forth the standards for applying compilation in classifying national security information.

Compilations of items of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that (1) meets the standards for classification under this order, and (2) is not otherwise revealed in the individual items of information. "Compilation" means an aggregation of pre-existing unclassified items of information.

The courts have applied the compilation theory most commonly in the national security area, where the courts have repeatedly stated that the "mosaic-like nature of intelligence gathering" often changes the way an agency will classify or protect information that seems otherwise innocuous.

**e) Discuss the classification authorities.**

Original classification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed. Derivative classification authority is granted for a period of 3 years. After 3 years, recertification is required if the authority is still needed.

**f) Discuss the classification guidance available within the DOE.**

Classification guidance contains detailed instructions for determining whether specific information is classified or unclassified. Examples of guidance include, but are not limited to, program guides, topical guides, local guides, bulletins, and change notices.

**g) Describe the classification/security markings placed on a classified document.**

*General Requirements*

Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD). Documents must be marked in accordance with directives in place at the time of origin or later, or in accordance with current directives. If there is a question about the classification level or category of a document, the document must be reviewed by a derivative classifier and re-marked (if necessary) to clearly indicate the level and category and to ensure proper protection. When possible, avoid returning documents because of improper markings. Instead, contact the sender and attempt to resolve any marking issues.

Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings, including declassification on a date or event, classification authority, or classifier's name, should be reviewed by a derivative classifier to ensure the classification level and category are still correct and then re-marked to bring them into conformance with current marking requirements. This must be done if the document is active or is to be transmitted outside of the organization for other than official archiving purposes. Documents created before April 1, 1996, need only contain classification level and category (if RD or FRD) to ensure proper protection.

Before using or distributing a document marked with the following obsolete markings, a derivative classifier or declassifier must determine the classification status and mark the document accordingly. DOE M 475.1-1A, Identifying Classified Information, provides requirements for reviewing and marking these documents. Pending review, documents must be handled and protected as C/NSI.

- Restricted. This is an obsolete U.S. classification marking used before December 15, 1953, that identifies a security level less sensitive than Confidential. This marking is still used by some foreign governments and international organizations.

- OUO. The Atomic Energy Commission used this term between July 18, 1949, and October 22, 1951, as an equivalent to the term Restricted. This marking is now used to identify unclassified information that may be exempt from disclosure under the FOIA.

*Markings*

The following elements are common to all classified documents: classification level, classification category (if RD or FRD), caveats and/or special markings (if required), classifier information, originator identification, classification of titles or subjects, unique identification numbers (if in accountability), and portion marking (if NSI). The DOE Marking Handbook provides guidance and examples for marking classified documents. The originator is responsible for ensuring that each classified document is marked correctly.

*Unique Identification Numbers*

Classified matter required to be in accountability must have a unique identification number. To ensure control and accountability of this matter, the unique identification number must be placed on the first page of paper documents and on the top or front of non-paper documents. The first page of a document is the first sheet of paper (i.e., the cover page, title page, or first page of text).

*Originating Organization and Date*

The name of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents. The first page of a document is the first sheet of paper, whether that is the cover page, title page, or first page of text. Classified documents being taken offsite must be marked on the first page to show the mailing address of the organization responsible for preparing the document. The mailing address should consist of a street address or post office box, city, state, and zip code. Note: When information cannot be accommodated on the first page, such as in the case of slides, microfiche, etc., this information must conspicuously accompany the classified document on a separate piece of paper.

*Classification Level*

The three classification levels, in descending order of sensitivity and potential damage to the National security, are Top Secret, Secret, and Confidential. Requirements for marking classified documents and materials are listed below:

- The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text.
- Each interior page of a classified document must be marked top and bottom with the highest classification level (or marked unclassified if applicable) of that page or the overall classification of the document.
- Classification markings must be clearly distinguishable from the document text.
- Classified material must have the classification level stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.

- Blank interior pages of a classified document need not be marked with the classification level or category or the notice "This page intentionally left blank."

*Classification Categories*

The three classification categories are RD, FRD, and NSI. Classified documents containing only NSI need not be marked with the NSI category marking. If the document is RD or FRD, the appropriate admonishment information must be marked on the first page of the document, whether that be the cover page, title page, or first page of text, and should appear in the lower left corner, as follows:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

FORMERLY RESTRICTED DATA
Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination per Section 144.b, Atomic Energy Act, 1954.

Each interior page of a document containing RD or FRD must be marked top and bottom with the appropriate level and category of information on that page. If this is not feasible, the overall level and category of the document (if RD or FRD) may be applied to every page. For interior pages, the symbols RD and FRD may be used. These markings must be clearly distinguishable from the document text.

Classified material (if RD or FRD) must have the classification category stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.

RD or FRD documents generated prior to July 9, 1998, will not be required to be re-marked to indicate the category on each page containing RD or FRD information unless they are sent outside the office of origin or holder for other than archiving purposes.

*Mixed Levels and Categories*

DOE policy states that matter must be classified and marked at the highest level and category of the information contained in it. When classified matter contains a mix of information at various levels and categories that cause the document to be marked at an overall level and category higher than the protection level required for any of the individual portions, a marking matrix may be used in addition to other required markings. This would allow access by an individual with a lower access level, such as an "L" cleared employee, to be given access to a document that they might not otherwise have been authorized to access if the document was only marked at the highest overall classification level and category. For example, a document that contains C/RD and S/NSI information would be required to be marked at the highest level and category, which is S/RD in this case, even though none of the information in the document is actually S/RD. However, this may not be interpreted to authorize any individual to gain access to information which exceeds their access authorization, formal access approvals, and "need to know." If a matrix is used, the following marking matrix, or one similar in content, will be used in addition to other required

markings, and must be placed on the first page of text. The marking should appear on the lower right corner near the classifier information marking. If the derivative classifier places this marking on the document at the time of the classification decision, there is no need to indicate the name and title of the derivative classifier on the mixed level and category marking. The derivative classifier's name and title are required only when a document is reviewed after the initial classification determination has been made and the mixed level and category marking is applied.

This document contains:
Restricted Data at the (e.g., Confidential) level.
Formerly Restricted Data at the (e.g., Secret) level.
National Security Information at the (e.g., Secret) level.
Classified by: Name and Title.

*Components*

When components of a document are to be used separately, each major component must be marked as a separate document. Components include annexes or appendices, attachments, and major sections of a report. If an entire major component is unclassified, "Unclassified" must be marked at the top and bottom of the first page and a statement included (e.g., "All portions of this [annex, appendix, etc.] are Unclassified."). When this method of marking is used, no further markings are required on the unclassified component.

*Unclassified Matter*

Unclassified matter need not be marked unless it is essential to convey one of the following conditions:

- The matter has been reviewed for classification and does not contain classified information.
- The matter has been properly declassified.

If unclassified matter is to be marked, the Unclassified marking must be placed on the top and bottom of the front cover (if any), title page (if any), and first page of text.

Unclassified information must not be marked in a manner that would be confused with markings specified for classified information (e.g., Confidential, etc.). If the unclassified matter carries a control marking (i.e., OUO, UCNI, or ECI), the information must retain its control marking; it should not be re-marked unclassified.

*Portions*

For NSI documents, each section, part, paragraph, graphic, figure, or similar portion of any such document dated after April 1, 1997, must be marked to show the classification level, or be identified as unclassified controlled information (e.g., UCNI, OUO) or as unclassified (U). Classification levels of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.

Page changes to NSI documents dated after April 1, 1997, must be portion marked. Additionally, any NSI document that becomes active (i.e., when sent outside the office of origin or holder other than for archival storage, or when removed from storage) must be

portion marked with the appropriate classification level, unclassified controlled symbol (e.g., UCNI, OUO, etc.), or unclassified. If any NSI document dated before April 1, 1997, is sent outside the office of origin or holder for other than archiving purposes, the entire document must be portion marked.

Documents containing RD or FRD are not required to be portion marked. However, in cases where portion markings are used, classification levels and categories (if RD or FRD) of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. Each section, part, paragraph graphic, figure, or similar portion of any such document must be accurately marked to show the following:

- The classification level and category (e.g., SRD or S/RD, CFRD or C/FRD, S, TS, etc.)
- That it is unclassified controlled information (e.g., UCNI, OUO)
- That it is unclassified (U)

Portion markings must include any applicable caveats.

Portions of U.S. documents containing FGI must be marked to reflect the foreign country of origin and appropriate classification level (e.g., U.K.-C, indicating United Kingdom-Confidential). FGI must be indicated in lieu of the country of origin if the foreign government indicates it does not want to be identified.

Classified documents generated by foreign governments do not require portion marking. Such documents generated and marked entirely by a foreign government must be protected commensurate with the level the foreign government specified.

Portions of U.S. documents containing NATO information must indicate NATO or COSMIC (NATO Top Secret documents), including the appropriate classification level (e.g., NATO-S or COSMIC-TS).

*Compilations*

In some instances, certain information that would otherwise be unclassified when standing alone may require classification when combined or associated with other unclassified information. When classification is required to protect a compilation of such information, the overall classification level and category (if RD or FRD) assigned to the document must be conspicuously marked or stamped at the top and bottom of each page, on the back of the last page of the document, and on the front cover, if any. A document classified for this reason is not required to be portion marked, but must contain the following statement on the first page: "This document has been classified under the compilation concept and shall not be used as the source for a derivative classification decision." The reason for classifying the information as a compilation also must be stated at an appropriate location near the beginning of the document.

*Subjects and Titles*

Except for extraordinary circumstances, unclassified subject descriptors and titles must be used for classified documents because they are used on mail logs, document receipts, and

other tracking or accountability records, most of which are entered into unclassified databases. Titles of classified documents must be marked even if the document is not portion marked.

If subjects or titles are classified, they must be marked with the appropriate classification level, category (if RD or FRD), and any applicable caveats. If titles are not classified, they must be marked as unclassified or with the appropriate unclassified controlled marking (e.g., OUO).

The classification or control symbols (e.g., U, OUO, UCNI, C/RD, S/FRD) must be placed immediately after the title or subject.

When classified documents with unmarked titles and/or subjects become active (i.e., sent outside the office of origin or holder, or removed from storage), the titles and/or subjects must be reviewed by a derivative classifier and marked appropriately.

If a caveat (e.g., ORCON) applies to the title or subject, it must be added to the title marking. A Secret NSI/ORCON title must be shown as S/ORCON.

*Authorized Markings for Portions, Subjects, and Titles*

The following are examples of the markings authorized for use with subjects and titles and when portion marking:

- Unclassified: (U)
- Official Use Only: (OUO)
- Unclassified Controlled Nuclear Information: (UCNI)
- Confidential National Security Information: (C)
- Confidential Formerly Restricted Data: (C/FRD) or (CFRD)
- Confidential Restricted Data: (C/RD) or (CRD)
- Secret National Security Information: (S)
- Secret Formerly Restricted Data: (S/FRD) or (SFRD)
- Secret Restricted Data: (S/RD) or (SRD)
- Top Secret National Security Information: (TS)
- Top Secret Restricted Data: (TS/RD) or (TSRD)
- Top Secret Formerly Restricted Data: (TS/FRD) or (TSFRD)

*Classifier Markings*

Classifier marking requirements can be found in DOE M 475.1-1A, Identifying Classified Information.

*Director of Central Intelligence Information*

The following markings, unless indicated otherwise, are authorized only for use for intelligence information:

- NOFORN. This marking indicates the information contained in the document may not be provided in any form to foreign governments, international organizations, coalition partners, foreign nationals, or immigrant aliens without originator approval. This marking may be used for intelligence information and NNPI only.
- ORCON. This marking indicates the document bearing the marking is controlled by the originator. Reproduction of, extraction of information from, or redistribution of such a document requires the permission of the originator. This marking must be used only on classified documents containing intelligence information that clearly

identifies, or would reasonably permit the identification of, intelligence sources or methods. It must not be used when access to the information can be reasonably protected by its classification markings or any other control markings. Without advanced permission from the originator, the dissemination of ORCON beyond the DOE Headquarters intelligence components and the formally designated field intelligence elements is limited. As a condition for receipt of ORCON by a non-intelligence component, written assurance that the recipient will observe the provisions of the Director of Central Intelligence Directive must be provided to the Office of Intelligence.

- PROPIN. This marking indicates the information contained in the document must not be released outside the Federal Government in any form to an individual, organization, or foreign government that has any interests, actual or potential, in competition with the source of the information without the permission of the originator of the intelligence information and provider of the proprietary information. This precludes dissemination to contractors, irrespective of their status within the Government, without the above consent.
- REL TO. This marking applies to intelligence information the originator has predetermined to be releasable or has released through established foreign disclosure procedures and channels to specified foreign countries or international organizations. The name of country or countries authorized access to the document must be included after the caveat (e.g., REL TO Canada, United Kingdom). The name of the country may be spelled out or abbreviated, but must be identifiable.

*Obsolete Markings*

The following markings are no longer used, but remain applicable on the documents that bear these markings until such time as the documents are re-reviewed and re-marked:

- No Dissemination to Contractors (NOCONTRACT)
- Warning Notice Intelligence Sources and Methods (WNINTEL)

Note: Existing instances of these markings remain valid until the documents containing them are re-reviewed and re-marked for classification purposes, or until they become declassified.

*Remarking Upgraded, Downgraded, and Declassified Matter*

When an official upgrade, downgrade, or declassification notice is received, the initial classification markings must be stricken and replaced with the new classification markings. The authority for and date of the upgrading, downgrading, or declassification notice must be entered on the first page of the document. The originator or document custodian must notify all known holders of the document.

Upgrading. A derivative classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of an upgrade notice from the proper authority. The originator or document custodian must notify all known holders with the proper access authorization when a document has been upgraded. Upon receipt of the authorization to upgrade a classified document, the first page of the document must be marked to show the date the classified document was upgraded and authority for upgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

Downgrading. A derivative declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of a downgrade notice from the proper authority. When the authorization to downgrade a classified document is received, the first page of the document must be marked to show the date the classified document was downgraded and authority for downgrading the document (e.g., a memorandum, an Office of Scientific and Technical Information notice).

**h) Discuss the authority and procedure to upgrade the classification of information and documents.**

A derivative classifier may upgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may upgrade its classification markings upon receipt of notice from the proper authority.

The derivative classifier authorizing the upgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being upgraded. The derivative classifier shall refer to appropriate classification guidance when preparing upgrading notices because such notices may be classified.

**i) Discuss the authority and procedure to reclassify information and documents.**

A derivative classifier may reclassify a document or material within his/her designated authority. The derivative classifier authorizing the reclassification of a document or material shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document or material being reclassified. The derivative classifier shall refer to appropriate classification guidance when preparing a reclassification notice because such notices are usually classified.

The public may request declassified documents under a statute or Executive order. Some of these documents may inadvertently still contain classified information. Such documents shall be referred to the Director of Nuclear and National Security Information, who shall review each one prior to its dissemination to determine if it may be reclassified. Documents containing only NSI that are more than 25 years old and that have been determined to be permanent records under Title 44 of the United States Code may not be reclassified under this provision.

**j) Discuss the classification status of research and development activities.**

An employee who develops a new, nuclear-related subject area that he/she believes may be classified shall request an evaluation of the subject area by the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements). The Director of Nuclear and National Security Information shall make a determination within 90 calendar days.

**k) Discuss the classification review of newly generated documents.**

Anyone who originates a document or material in a subject area that may be classified shall submit the document or material to the appropriate official for a classification review and determination prior to dissemination.

**l) Discuss the declassification and downgrading of classified information and documents.**

*Declassification*

A derivative declassifier may derivatively declassify a document or material originated in only those organizations and subject areas for which he/she has been delegated such authority, and is governed by other limitations specified in the written designation. A derivative declassifier shall base his/her determinations on classification guidance pertaining to the specific subject areas described in the declassifier's designation of authority.

*Review Requirements for Redacting a Document or Declassifying a Document or Material*

Preparing a redacted version of a document (i.e., a version of the document with all classified information removed) or declassifying a document or material in full requires two reviews by individuals who are knowledgeable in the subject area. The first review may be conducted by either a derivative classifier or declassifier. The second review shall be conducted by a derivative declassifier (other than the first reviewer), who shall confirm that all classified information has been identified and bracketed in the document to be redacted, or that the declassified document or material is unclassified.

*Required Markings*

For each document or material that is declassified, the derivative declassifier shall ensure that the following markings are included on the document or material and that the classification markings are crossed out:

- Date of declassification (i.e., "Declassified On")
- Name(s) and position(s) or title(s) of individual(s) declassifying the document (i.e., "Declassified By")
- Designation of the guidance or source document(s) used as the basis for the declassification determination and the date of such document(s) (i.e., "Derived From")

*Downgrading*

Downgrading occurs when an appropriate authority determines the document or material can be adequately protected at a classification level or category lower than currently marked, but not including "Unclassified."

A derivative declassifier may downgrade the classification of a document or material within his/her designated authority. The custodian of a document or material may downgrade its classification markings upon receipt of notice from the proper authority.

The derivative declassifier authorizing the downgrading of a document shall notify the originator or document custodian and provide sufficient information for the originator or document custodian to identify the specific document being downgraded.

**m) Discuss the policy, objectives, standards, and procedures for conducting classification appraisals.**

Classification and declassification programs at various facilities differ in scope and complexity. No single list of areas to be covered in an oversight review is appropriate in all cases. Therefore, the scope of the oversight review must be tailored to ensure that it provides the management and oversight necessary to evaluate the adequacy and effectiveness of each individual classification and declassification program.

To introduce a measure of uniformity into classification and declassification oversight reviews, each review shall cover, at a minimum, the following areas:

- Management awareness and support
- Document reviews
- Guidance
- Education
- Classifiers and declassifiers
- Declassification
- Effectiveness of the program to publicly release declassified documents
- Oversight reviews of contractors

*Frequency of Oversight Reviews*

The frequency of oversight reviews is determined after considering the following factors:

- Past Performance Experience and Review Results. More frequent reviews are conducted of facilities that have experienced problems previously.
- Interval Since Last Review. Facilities having a major classification and declassification interest are reviewed every 2 years unless particular circumstances indicate otherwise. Facilities with effective classification and declassification programs or minor interests may be reviewed less frequently (every 3-5 years). The local classification officer shall determine the frequency of oversight reviews of subordinate facilities.

*Oversight Review Reports*

The oversight review report shall ensure the organization reviewed receives a clear explanation of its performance. The review report shall ensure that deficiencies or problem areas are identified.

*Follow-Up Measures*

Follow-up measures shall ensure that the actions taken to correct deficiencies noted during an oversight review are adequate and have been implemented in a timely manner.

*Self-Assessments*

Each DOE, including NNSA, element that generates classified information and documents or material shall establish and maintain an ongoing self-assessment program, documented in writing to the Director of Nuclear and National Security Information (through the Chief of Defense Nuclear Security for NNSA elements). Self-assessments shall be conducted annually unless prior agreement is reached with the Director of Nuclear and National Security Information.

**n) Explain the relationship between DOE Manual 475.1-1A, Identifying Classified Information; Executive Order 12958, National Security Information; 32 CFR 2001, National Security Information; and the Atomic Energy Act of 1954 as amended, with respect to classified information.**

All of these documents provide information on the classification process used by DOE.

**30. Safeguards and security personnel acting in information security shall demonstrate the ability to assess the contractor's classified computer security programs in accordance with DOE Order 471.2A, Chapter III, Classified Information Systems Security, and DOE Manual 471.2-2, Manual of Security Requirements for the Classified Information System Security Program.**

**a) Assess the contractor's management and planning programs for computer security.**

**b) Assess the contractor's program for the protection of information assets.**

**c) Assess the contractor's programs for the physical protection of computing resource assets.**

**d) Assess of the contractor's programs that ensure continuity and reliability of operations.**

Elements "a" through "d" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**31. Safeguards and security personnel acting in information security shall demonstrate the ability to assess the effectiveness and efficiency of the local organization's management program in meeting security objectives for information security.**

**a) Assess the contractor's procedures for document and material control.**

**b) Assess the contractor's self-inspection program for information security.**

**c) Perform a Foreign Ownership, Control, or Influence (FOCI) determination of a contractor.**

Elements "a" through "c" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**32. Safeguards and security personnel acting in information security shall demonstrate the ability to assess the contractor's control of Top Secret, Secret, and Confidential documents in accordance with DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M 5632.1C -1, Manual for Protection and Control of Safeguards and Security Interests.**

**a) Assess the contractor's practices during all phases of the control and use of Secret and Confidential matter.**

**b) Assess the contractor's practices during all phases of the control and use of Top Secret matter.**

**c) Given a hypothetical security infraction, simulate the process of reporting and disposing of the infraction.**

Elements "a" through "c" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**33. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the DOE Safeguards and Security program.**

**a) Define the terms safeguards and security as they apply to the DOE. Provide examples of each.**

*Safeguards*

Safeguards consist of an integrated system of physical protection, material accounting, and material control measures designed to deter, prevent, detect, and respond to unauthorized possession, use, or sabotage of nuclear materials.

*Security*

Security is an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information and/or classified matter, unclassified controlled information, nuclear materials, nuclear weapons, nuclear weapon components, and/or the Department's and its contractors' facilities, property, and equipment.

**b) Describe the major safeguards and security objectives within the Department.**

The major safeguards and security objectives within the Department are to establish a standardized approach for protection program planning that will provide an information baseline for use in integrating Departmental S&S considerations, facilitating management evaluation of program elements, determining resources for needed improvements, and establishing cost-benefit bases for analyses and comparisons.

**c) Describe the major elements of the DOE's Safeguards and Security program.**

Following are essential elements for planning for S&S programs.

*S&S Philosophy*

S&S interests and activities must be protected from theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security or the environment, or that pose significant danger to the health and safety of DOE federal and contractor employees or the public.

*S&S Management Plan*

An S&S management plan must provide a description of the implementation of S&S policy and provide detailed information on the assignment of roles, responsibilities, and authorities,

as well as the development of budgets and the allocation of resources. The S&S management plan must be updated annually (at least every 12 months) and must document

- roles, responsibilities, delegations, and authorities for the S&S program;
- organizational structure and accountability;
- planning and budget (including personnel resources).

*S&S Program Operations*

Actions must be taken to ensure an acceptable S&S program, including curtailment or suspension of operations when such operations would result in an immediate and unacceptable impact to national security, the environment, or the health and safety of the public or employees.

*Graded Protection*

The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for, or consequences of, all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

*Risk Management*

S&S programs must be based on the results of vulnerability and risk assessments, the results of which are used to design and provide graded protection in accordance with an asset's importance or the impact of its loss, destruction, or misuse. The results of the assessments, to include the determination of system effectiveness, are one of the key considerations the manager must evaluate when establishing the level of risk. For example, if it is determined that there is high risk that is not being mitigated by compensatory measures, reporting must be made to the Secretary of Energy or the Deputy Secretary who can accept high risk. cognizant Under Secretaries can accept moderate risk.

**d) Describe the objective of Integrated Safeguards and Security Management (ISSM).**

A principal objective of the ISSM Program is to integrate S&S into management and work practices at all levels, based on program line management's risk-management-based decisions, so that missions may be accomplished without security events, such as interruption, disruption, or compromise.

**e) Describe the levels of access authorization used within the DOE.**

The levels of access authorization used within the DOE are "Q" and "L."

A Q access authorization must be requested when the duties of the position require access to any of the following:

- Top Secret or Secret Restricted Data
- Top Secret Formerly Restricted Data
- Top Secret National Security Information

- Classified information or matter designated as "COMSEC," "CRYPTO," "Sensitive Compartmented Information," or Weapon Data, Sigma 14 or Sigma 15
- SNM designated as Category I, and other categories with credible roll-up to Category I

Note: A Q access authorization also authorizes the individual access to the categories/levels of classified information or matter listed for L clearances, below.

An L access authorization must be requested when the duties of the position require access to any of the following:

- Confidential Restricted Data
- Secret or Confidential Formerly Restricted Data
- Secret or Confidential National Security Information
- SNM designated as Categories II and III, unless special circumstances determined by a site vulnerability assessment and documented in the Site Safeguards and Security Plan (SSSP) or Site Security Plan (SSP) require a Q access authorization

**f) Describe the graded approach policy.**

The Department recognizes that risks must be accepted (i.e., that actions cannot be taken to reduce the potential for, or consequences of, all malevolent events to zero); however, an acceptable level of risk must be determined based on evaluation of a variety of facility-specific goals and considerations. By a graded approach, the Department intends that the highest level of protection be given to security interests and activities whose loss, theft, compromise, and/or unauthorized use would seriously affect the national security, the environment, Departmental programs, and/or the health and safety of the public or employees. Protection of other interests and activities must be graded accordingly.

**34. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of threat awareness.**

**a) Discuss the following terms:**

- **Abrupt theft**
- **Protracted theft**
- **Diversion**
- **Radiological sabotage**
- **Toxicological sabotage**
- **Industrial sabotage**
- **Espionage**

*Abrupt Theft or Diversion*

An abrupt theft or diversion is one that is accomplished during a single occurrence.

*Protracted Theft or Diversion*

A protracted theft or diversion is one that is accomplished by repeated occurrences.

*Diversion*

A diversion is

- the unauthorized removal of nuclear material from its approved use or authorized location
- an act that attempts to reposition the PF to a location other than where the actual adversarial action is taking place

*Radiological, Chemical, or Biological Sabotage*

Physical protection strategies must be developed, documented, and implemented consistent with the DBT to protect radiological, chemical, or biological sabotage targets:

- Radiological. Targets must be protected in a graded manner to protect S&S interests and to mitigate consequences of a radiological sabotage event.
- Chemical. Targets must be protected to protect S&S interests and to mitigate consequences of a chemical sabotage event.
- Biological. Targets must be protected to protect S&S interests and to mitigate consequences of a biological sabotage event.

*Espionage*

Espionage is the systematic use of spies to get military or political secrets.

**b) Discuss the protection strategies of denial and containment.**

The basic strategies pertaining to protection are denial of access, denial of task, and containment that upon failure could evolve into recapture/recovery or pursuit strategies.

Denial is the effect achieved by S&S systems or devices that prevents a potential intruder or adversary from gaining access to, or use of, a particular space, structure, facility, or asset.

Containment is the effect achieved by S&S systems and personnel that prevents an adversary or SNM from leaving a particular space, structure, or facility.

A denial strategy is implemented as follows:

- Early warning system technologies are emplaced to detect and to assess adversary movement as far as possible from target locations.
- Highly mobile tactical vehicles (armored and/or unarmored) mounted with light and/or heavy weapon systems are deployed to support combat operations, conduct reconnaissance operations, control avenues of approach, maneuver to suppress and destroy hostile threats, and provide mutual support for other tactical vehicles.
- A commander is designated for each tactical armored vehicle (for a two-person crew, the commander is usually the gunner).
- Potential target access points are covered by suppressive fire weapons.
- TRF members utilize positions of cover and maximize the element of surprise to the extent possible.
- The TRF initiates a decisive engagement with adversary forces as far as possible outside the target location.
- Once an adversary has been identified and engaged, TRF elements never lose contact.
- Adversaries are engaged while they negotiate obstacles (i.e., fences, barriers), deploy from vehicles (both airborne and ground based), and cross open ground.

- TRF teams, using suppressive fire weapons, maneuver in force against adversaries occupying covered positions.
- The TRF has plans in place to transition quickly from defensive to offensive operations.

**c) Discuss the basic adversary types recognized as a DOE threat.**

An adversary is any government, organization, group, or individual whose interests are adverse to those of the U.S. Government in general and to those of the Department in particular.

**35. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the Design Basis Threat Policy for the DOE Programs and Facilities.**

**a) Describe how the design basis threat is used in safeguards and security planning.**

DOE O 470.3, Design Basis Threat Policy, must be used with local threat guidance during the conduct of VAs for protection and control program planning. The DBT must be the baseline threat definition, but local threat guidance may be used to increase the level of threat to be analyzed.

Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and specific threat indicators. Threat indicators should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of threat indicators that can be used to develop a site-/facility-specific assessment are listed below:

- International incidents or indicators against U.S. interests, personnel, or facilities
- Domestic incidents or indicators against federal or state interests countrywide
- Local incidents or indicators directed against federal or DOE interests
- Specific targeting of DOE personnel, facilities, or materials

Note: DOE O 470.3, Design Basis Threat Policy (U), is a classified order and must be requested through DOE Headquarters.

**b) Describe the method used to identify and characterize the range of potential adversary threats.**

*Threat Indicators*

While the DBT provides specific descriptions of threats that all components of the S&S system must be capable of defeating, analysis of terrorism should be an ongoing process. Although each analysis relies on information included in previous assessments, judgments with respect to threats to federal and DOE-affiliated personnel, facilities, and assets begin anew with each analysis.

**c) Discuss the responsibilities of safeguards and security personnel in the development of a design basis threat.**

Local and site-specific threat analysis is a dynamic process because the threat and the countermeasures used to combat the threat are constantly changing. To keep up with possible changes in the threat, security professionals should develop a predetermined list of general and

specific threat indicators. Threat indicators should be revised according to site/facility situations and needs. They should be reviewed at least every 6 months or when a significant incident or change in conditions indicates that the threat level is increasing or decreasing. Examples of threat indicators that can be used to develop a site-/facility-specific assessment are listed below:

- International incidents or indicators against U.S. interests, personnel, or facilities
- Domestic incidents or indicators against federal or state interests countrywide
- Local incidents or indicators directed against federal or DOE interests
- Specific targeting of DOE personnel, facilities, or materials

**36. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the planning process described in DOE O 470.1, Safeguards and Security Program.**

Note: DOE O 470.1, Safeguards and Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management.

**a) Discuss the contents of the Site-Specific Security Plan, Facility Descriptions and Operational Plans and the interrelationship between them.**

*Site-Specific Security Plan*

The SSSP is a risk management document that provides summary information used to describe S&S programs and vulnerability and risk assessments at applicable sites. The results and conclusions contained in the plan are intended to guide long-term planning for site S&S operations. This is accomplished during plan development by identifying key site protection elements, annually (at least every 12 months) evaluating site protection in terms of its adequacy to meet continued mission and threat parameters, and identifying resource requirements. The SSSP is used to evaluate site and facility program elements and resources as they relate to identified threats and risks. The protection measures identified in approved SSSPs become the basis for executing and reviewing site protection programs.

The SSSP includes

- references to implementing documents and evidence files;
- descriptions of site protection strategies, key site S&S programs, approved and pending deviations, and plans and procedures designed to implement, manage, and maintain S&S programs;
- system effectiveness determinations for the protection of SNM, prevention or mitigation of sabotage events, and prevention and/or timely detection of the loss of classified information or matter based on the status of performance indicators, such as results of VAs, performance tests, surveys, inspections, and evaluations of personnel qualifications and training;
- proposed S&S program upgrades;
- VAs results that support conclusions reported in the SSSP;
- assumptions used as part of the VA process;
- threat parameters used for VAs that are described in the current DBT, regional threat assessments, and impacts made by local area threat assessments, if applicable;
- the details of the changes in the protection through the spectrum of Security Conditions (SECON) (1-5), to include effects on the calculated baseline system effectiveness;
- a description of the evidence files containing material that supports the VAs;

- a resource plan (RP) that describes S&S upgrades programmed for completion, upgrades being introduced as a result of planned and unplanned site changes impacting the protection program or deficiencies identified as a result of the annual (at least every 12 months) review of the SSSP, a description of the funding source to implement the upgrades, and unfunded requirements.

S&S program planning and management must be integrated with other programs such as physical protection, PF, information security, personnel security, and nuclear material control & accountability (MC&A). Mechanisms must also exist to assure that S&S program planning is fully integrated with overall site strategic and near-term operational planning. Additionally, the activities and requirements in the weapons surety, foreign visits and assignments, safety, emergency management, cyber security, and intelligence and counterintelligence programs should also be considered in the implementation of this Manual.

**b) Discuss the processes for reviewing and validating site-specific security plans, facility descriptions, and operational plans.**

*SSSP Plan Review and Approval*

The SSSP requires approval by DOE line management and concurrence by the cognizant head of the Departmental element. Such approval authority must be formally delegated to line management. Copies of approved SSSPs must be provided to the Office of Security for review and comment. Other security plans may be approved as stipulated in the applicable directive. If approving authority is not otherwise stipulated, these security plans may be approved by DOE line management.

The SSSP must be submitted to DOE line management within 150 days of the termination date of data collection and approved within 120 days of the submittal date. Directive changes, facility reconfiguration, a new VA, or other activities that occur after the stated effective date will not be considered for purposes of reviewing/approving the plan.

The SSSP must be reviewed annually (at least every 12 months). Updates to the SSSP that may significantly alter the agreed-upon protection philosophy or performance standards of protection systems must be subjected to the formal VA process.

An information copy of approved modifications must be provided to the Office of Security.

**c) Discuss the resources necessary to develop a site safeguards and security plan including necessary site documentation and on-call expertise.**

The SSSP RP identifies S&S resources necessary to ensure protection of Department assets and identifies changes in resource requirements (i.e., operational requirements, capital equipment, general plant projects, and line item construction projects that directly impact risk, indirectly impact risk, or derive from changing S&S policy, directives, guidance, or other Departmental direction).

Operational requirements must include, but are not limited to, material consolidation, facility mission changes, changes in the DBT impacting site operations, PF redeployments, maintenance and testing changes, PF manning levels, procuring technical expertise and support personnel, and additional training requirements.

**37. Safeguards and security personnel shall demonstrate a working-level knowledge of DOE O 470.1, Safeguards and Security Program.**

Note: DOE O 470.1, Safeguards and Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management.

**a) Assess the facility's acceptance and validation test for safeguards and security that validate functional requirements and effectiveness of safeguards and security elements that have been implemented and are operating as part of a total system.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**b) Assess the contractor's ability to identify and test critical system elements during acceptance and validation tests.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**c) Discuss the required frequency of performance testing.**

At least every 365 days, an integrated performance test encompassing all essential protection elements associated with a comprehensive site or facility threat scenario must be conducted to evaluate the overall facility S&S effectiveness.

- Those Category I facilities requiring denial protection strategies must conduct integrated performance testing on a quarterly basis (at least every 3 months).

OR

- Those sites with multiple Category I facilities requiring denial protection strategies may rotate quarterly performance testing so that at least one facility is tested on a quarterly basis (at least every 3 months). However, an integrated performance test for all Category I facilities must occur at least once every 365 days.

**d) Describe the required sections of the safeguards and security acceptance and validation test program plan.**

A documented and formalized safeguards and security acceptance and validation test program plan should be developed for each facility and should be included as part of the approved safeguards and security plan. The purposes of this program plan are to document the process and to identify a comprehensive set of tests and a frequency of testing which confirm the ability of an implemented and operating critical system element or total system to meet requirements contained in DOE safeguards and security Orders and Manuals. The plan should include the following sections as a minimum:

- Program Description. A description of the facility's safeguards and security acceptance and validation testing program should be provided. Descriptive elements should include the development, implementation, revision, and recordkeeping of test plans, and the preparation of required reports.

- Program Administration. A description of organizations and positions responsible for developing, implementing, and maintaining test plans and submitting reports should be included in this section.
- Critical System Elements. The requirements basis consisting of critical system elements to be confirmed through testing should be described and listed in this section.
- Test Documentation Requirements. A list of test plans and test reports should be included in this section, with a reference to each requirement presented in the Critical System Elements section.
- Corrective Action Requirements. Corrective actions to be taken for failures of safeguards and security elements to pass test criteria specified as a requirements basis should be described in this section.
- Resources. Specialized personnel, equipment, and facilities required for development, implementation, revision, and archival of the test program should be identified and described in this section.
- References. A list of pertinent requirements basis documents, standards, procedures, and reports should be included in this section.

**e) Describe the required sections of the safeguards and security validation test plan.**

Written test plan(s) should be developed for each facility to validate safeguards and security systems and critical elements. The plan should include the following sections at a minimum:

- Test Objectives. Identify and describe the test objectives.
- Scenario Description(s). Describe the threat scenarios evaluated by the validation tests. The scenarios may be restricted to specific, limited aspects of the safeguards and security system (e.g., weapons detection at a Protected Area entry point, or many elements of a total system, such as a Force on Force exercise).
- Test Methodology and Evaluation Criteria. State how the validation test will be conducted. List the steps involved in the process of planning and execution. Include a description of any statistical models or mathematical formulas used to determine probabilities and confidence levels, the number of tests to be performed under each scenario to be tested, and pass/fail criteria. Also, models, equations, or methods to be used for data analysis should be presented and discussed in detail. For tests validating effectiveness of equipment, provisions for recording calibration settings and equipment configurations should be described.
- Test Controls. Identify those controls to be imposed to maintain the integrity of the test, yet minimize safety and security risks. Controls apply to people, procedures, and equipment characteristics (e.g., use of trusted agents, providing minimum notice of testing, controlling lighting levels, or testing equipment under specific temperature and humidity environmental conditions).
- Resource Requirements. List resources that are needed to effectively conduct the test, including facilities, personnel, and equipment.
- Test Coordination Requirements. Identify operational and support elements such as facility operations, safety, quality assurance, and safeguards and security management, where coordination is necessary.
- Operational Impact(s) of the Testing Program. Describe the operational impacts, if any, that will result from conducting the test (e.g., facility production rates and overtime costs).

- Compensatory Measures (if necessary). Identify measures that are necessary to compensate for any degradation of safeguards and security readiness experienced while conducting the validation test. Also, identify measures to be implemented in the event of test failures. Reference to existing approved procedures for compensatory measures is acceptable.
- Coordination and Approval Process. Describe the approval and signoff process for test records and reports, including provision for witness initials, dates of data collection, and use of compensatory measures.
- References. Applicable DOE Orders and Manuals, SSSPs, Safeguards and Security plans, and other DOE policy related documents containing requirements for the element or system being validated should be included in a list of references. Also, any other reference material used in analysis, calculations, or discussion in this test plan or the associated test report shall be included in this list. For each reference, applicable sections and/or paragraph numbers should be included.

**f) Discuss the required sections of the safeguards and security acceptance and validation test reports.**

Test results should be documented in test reports that should include the following sections at a minimum:

- Objectives. A restatement of test objectives from the associated test plan should be included to permit a basic understanding of the data collected and the significance of the conclusions and recommendations.
- Test Data. Recorded test data should be provided, including test forms and data sheets with original signoffs and handwritten notes. Test data, signoffs, and dates beside each signoff shall be recorded in pen and ink.
- Data Analysis. Analysis of the test data should be documented using models, equations, or the methodology presented in the associated test plan.
- Test Results and Recommendations. A statement of success or failure according to evaluation criteria provided in the test plan should be included. Also, any unusual observations related to the area tested, but not otherwise addressed in the associated test plan, should be discussed. Recommendations should be included for any variations from expected test results.
- Corrective Actions. Corrective actions recommended for safeguards and security measures failing to meet requirements should be listed and discussed. The persons, organizations, or groups responsible for the corrective actions should be identified. Both immediate and longer range solutions will be discussed.
- References. The related test plan and other pertinent references included in the test plan should be listed.

**g) Describe what determines unsatisfactory test results and how these are resolved.**

Unsatisfactory means that the element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

*For Notifications and Actions for Less Than Satisfactory Survey Composite Ratings*

Within 24 hours of determination of an overall composite rating of Unsatisfactory, the DOE cognizant security authority must coordinate with the Departmental element to suspend the

activity and/or the Facility Clearance (FCL) pending remedial action, or provide the justification for continuing this critical operation to the Office of Security, the Departmental element, and as directed, other applicable Departmental elements. In addition to providing the rationale, the DOE cognizant security authority must identify and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

If the surveying office is not the same as the DOE cognizant security authority, the surveying office must notify the DOE cognizant security authority of the results immediately. If the surveying office is unable to contact the DOE cognizant security authority, action must be taken to protect activities until the DOE cognizant security authority can be notified. Subsequent action must be taken on the basis of agreement between the two organizations and must be fully documented in the survey report.

*For Self-Assessments*

Within 24 hours of determination of an overall composite rating of Unsatisfactory, the cognizant security authority must coordinate with the DOE cognizant security authority, which in turn must coordinate with the Departmental element to suspend the activity and/or recommend suspension of the FCL pending remedial action, or provide justification for continuing operations to the DOE cognizant security authority. In addition to providing the rationale, the cognizant security authority must evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

**38. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of DOE O 470.1, Safeguards and Security Program, and DOE G 470.1-2, Safeguards and Security Self-Assessment Guide.**

Note: DOE O 470.1, Safeguards and Security Program, and DOE G 470.1-2, Safeguards and Security Self-Assessment Guide, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management.

**a) Discuss the responsibilities and authorities of the heads of Field elements.**

*Heads of Field Elements*

Heads of field elements must review procurement requests for new non-site-/non-facility-management contracts that involve classified information or matter or nuclear materials, and that are subject to DEAR clause 952.204-2, titled Security Requirements. If appropriate, they must ensure that the requirements of the CRD of DOE M 470.4-1 are included in the contract.

Delegations must be documented in writing and must delineate all assigned S&S roles, responsibilities, and authorities for the S&S program.

**b) Describe the facility importance rating and approval systems.**

Importance ratings are used to identify the protection importance of facilities. Each facility's assigned importance rating must be recorded on DOE F 470.2, FDAR. Importance rating criteria are addressed below.

"A" importance ratings are ratings assigned to those facilities that

- are engaged in administrative activities considered essential to the direction and continuity of the overall DOE nuclear weapons program, as determined by the Departmental element;
- are authorized to possess Top Secret or that possess SAP matter, or that are designated as field intelligence elements;
- are authorized to possess Category I quantities of SNM (including facilities with credible roll-up quantities of SNM to a Category I quantity);
- have critical infrastructure programs determined to be essential by DOE line management.

"B" importance ratings are ratings assigned to those facilities that are

- engaged in activities other than those categorized as "A" and are authorized to possess Secret (S)/Restricted Data (RD) and/or weapon data matter;
- authorized to possess Category II quantities of SNM;
- authorized to possess certain categories of biological agents.

"C" importance ratings are ratings assigned to those facilities that are

- authorized to possess Categories III and IV quantities of SNM, or other nuclear materials requiring safeguards controls or special accounting procedures;
- authorized to possess classified information or matter other than the type categorized for "A" and "B" facilities.

"D" importance ratings are ratings assigned to those facilities that provide common carrier, commercial carrier, or mail service and are not authorized to store classified information or matter or nuclear material during nonworking hours. (Carriers who store classified information or matter or nuclear material must be assigned an "A," "B," or "C" importance rating.)

"E" importance ratings are ratings assigned to a corporate tier parent (of a contractor organization) that has been barred from participation in the activities related to a contract with DOE.

"PP" (Property Protection) importance ratings are ratings assigned to those facilities for which a special standard of protection must be applied. Basic considerations include physical protection to prevent or deter acts of arson, civil disorder, riots, sabotage, terrorism, vandalism, and theft or destruction of DOE property and facilities. These special standards are applied when a facility has

- Government property of a significant monetary value (more than $5 million, exclusive of facilities and land values);
- nuclear materials requiring safeguards controls or special accounting procedures other than those categorized as types "A," "B," or "C";
- responsibility for DOE program continuity;
- national security considerations;
- responsibilities for protection of the health and safety of the public and employees.

"NP" (Non-Possessing) importance ratings are ratings assigned to those facilities that have authorized access to classified information or matter or SNM at other approved locations. Non-possessing facilities do not themselves possess any classified information or matter or SNM.

**c) Describe the general survey requirements.**

Surveys are conducted by the DOE cognizant security authority.

*Types and Frequencies of Surveys and Assessments*

Initial Surveys. Initial surveys must be conducted at facilities where there will be a facility clearance established for a facility with an importance rating of A, B, C, or PP. Survey activities must be comprehensive and result in a satisfactory composite rating prior to a facility clearance being granted.

Periodic Surveys. Periodic surveys are conducted for all facilities and must cover all applicable topics to ensure survey program objectives are met. The periodic survey may be composed of multiple special survey reports, providing all the requirements of this section are met. Integration of internal and external reports including quality assurance, property appraisals, performance assurance, and other evaluation reports may be used to augment the requirement for a periodic survey.

Special Surveys. Special surveys may be conducted at facilities for specific limited purposes. Examples include extended survey activities, technical security activities, "for cause" reviews, line management direction, shipment of nuclear and/or classified information or matter, or a change in the contractor operating a Government-owned facility.

Termination Surveys. Termination surveys must be conducted to verify the termination of Departmental activities and appropriate disposition of S&S interests. Examples of survey activities include: the appropriate disposition, destruction, or return of classified information or matter, SNM, hazardous material, or property; security badge retrieval; debriefings; and verification of the termination or transfer of DOE access authorizations.

Periodic Reviews. A documented review of entities (D, NP, and E facilities) such as subcontractors, consultants, and common carriers must be performed by the DOE cognizant security authority at least every five years.

Self-Assessments. Contractors must conduct self-assessments between periodic surveys conducted by the cognizant security authority and must include all applicable facility S&S program elements. The self-assessment must ensure the S&S objectives are met. Note: NP facilities are not required to conduct self assessments. However, sponsoring organizations (federal or contractor) must include in their self-assessments a thorough review of their registration program for NP facilities which may result in a program review of identified subcontractors.

Reviews or Inspections by Other DOE Elements or OGAs. Reviews/inspections conducted by other DOE elements (including site quality assurance programs) or OGAs may be used to meet survey requirements.

Extension of Frequency. The results of previous surveys may affect the frequency of future surveys. Contractors may request that the interval between periodic surveys be increased up to 24 months by the DOE cognizant security authority. Documentation of the justification for increases in the interval of periodic surveys must be maintained by the DOE cognizant security authority.

**d) Describe the process for conducting safeguards and security surveys.**

Local survey and self-assessment procedures must be developed, documented, and approved by the cognizant security authority. Procedures must include the requirements listed below:

- Team Composition. Contractor line management must determine that contractor survey and self-assessment team members possess qualifications, experience, and training sufficient to review and inspect the topical/subtopical areas of survey/ self-assessment. The National Training Center provides training courses for survey/ self-assessment team leaders and team members.
- Planning, Scheduling, and Integration. Surveys and self-assessments must be planned, scheduled, and conducted in an integrated manner. If topical and subtopical area evaluations are performed separately, the surveying office must document and integrate the results of each into a single (periodic) survey report that includes a composite facility rating. The frequency between topical and subtopical areas cannot exceed the frequency for the single (periodic) survey.
- Validation. Results must be validated by methods including, but not limited to, document review, performance testing, and interview analyses and observations.
- Exit Briefing. An exit briefing must be conducted with the surveyed or assessed organization to include the minimum facts:
  - Program strengths and weaknesses, including all findings
  - Corrective action reporting requirements for all open findings, regardless of source
  - Topical and composite ratings

**e) Describe the actions systems for survey ratings and follow-up.**

*Ratings*

Ratings must be based on the effectiveness and adequacy of the program at a facility and must reflect a balance of performance and compliance results as well as the impact of the deficiency(ies) (e.g., findings, IG recommendations) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. "Does not apply" (DNA) and "Not Rated" (NR) may also be used in applicable situations.

The Types of ratings are as follows:

- Satisfactory. The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.
- Marginal. The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.
- Unsatisfactory. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.

- Inspection Ratings. "Effective Performance," "Needs Improvement," and "Significant Weaknesses" are indicators of a management system performance level as outlined in DOE O 470.2B, Independent Oversight and Assurance Program.

*Rating Determinations*

Existing Conditions. Ratings must be based on existing conditions at the end of the survey and not on future or planned corrective actions or conditions.

Impact. Ratings must be based on the impact of all open deficiencies, regardless of source.

Marginal or Unsatisfactory Ratings. Less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&S system or on deficiencies in performance.

Topical Area Ratings. A topical area rating must not be marginal for consecutive survey periods and must be assigned an unsatisfactory rating unless one of the following conditions applies:

- The current survey of the topical area results in a satisfactory rating.
- The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.
- The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a line item construction project or upgrade program. (In this case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.)

Subtopical Ratings. The decision whether or not to use all subtopical ratings must be documented in local procedures. Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.

Justification and Rationale. All ratings must be supported and documented to include the rating justification and rationale.

*Notifications and Actions for Less Than Satisfactory Survey Composite Ratings*

When the survey composite ratings are less than satisfactory, the following notifications and actions must occur:

- Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, the DOE cognizant security authority must ensure SSIMS is updated and must provide the applicable Departmental elements and OGAs with the following:
  - A statement identifying the vulnerabilities and the rationale for the rating
  - A description of the corrective action/compensatory measures taken to date
  - A statement acknowledging physical validation of the adequacy of items
- Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of Unsatisfactory, the DOE cognizant security authority must coordinate with the Departmental element to take one of the following actions:
  - Suspend the activity and/or the FCL pending remedial action.
  - Provide the justification for continuing this critical operation to the Office of Security, the Departmental element, and as directed, other applicable Departmental elements, and identify and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

*Notification and Action for Less Than Satisfactory Self-Assessment Composite Ratings*

Actions required in response to less than satisfactory self-assessment composite ratings are listed below:

- Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, notification must be made to line management that includes the following:
  - A statement identifying the vulnerability and rationale for the rating
  - A description of the corrective action/compensatory measures taken to date
  - A statement acknowledging physical validation of the adequacy of items
- Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of unsatisfactory, the cognizant security authority must coordinate with the DOE cognizant security authority, which in turn must coordinate with the Departmental element to take the following actions:
  - Suspend the activity and/or recommend suspension of the FCL pending remedial action.
  - Provide justification for continuing operations to the DOE cognizant security authority, and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.
  - If the results of a self-assessment identify an incident of security concern, it must be reported in accordance with Section N of this CRD.

*Corrective Actions*

Corrective action plans must be developed for all open survey and self-assessment findings. Corrective action plans for survey and self assessments must be submitted and reported within 30 working days after the date of the exit briefing. If a finding is corrected during the survey, it must be identified in the survey report with a description of the closure/validation performed by the survey/self assessment team. Quarterly reports of the status of corrective actions for each finding must be provided to the DOE cognizant security authority.

**39. Safeguards and security personnel shall demonstrate a familiarity level of knowledge of the programs outlined in DOE O 471.2A, Chapter II, Operations Security Program.**

Note: DOE O 471.2A, Chapter II, Operations Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-4, Information Security, and DOE M 470.4-7, Safeguards and Security Program References.

**a) Describe the Department's Operations Security (OPSEC) program structure.**

OPSEC is a process designed to disrupt or defeat the ability of foreign intelligence or other adversaries to exploit sensitive Departmental activities or information and to prevent the inadvertent disclosure of such information.

*OPSEC Objectives*

The objectives of OPSEC are to

- help ensure that Critical Program Information (CPI), including unclassified controlled information, is protected from inadvertent and unauthorized disclosure;

- provide management with the information required for sound risk management decisions concerning the protection of sensitive information;
- ensure that OPSEC techniques and measures are used throughout the Department.

*OPSEC Requirements*

An OPSEC program must be implemented to cover each program office, site, and facility to ensure the protection of classified and unclassified controlled information. The OPSEC program must also include the following activities:

- Establish a designated point of contact with overall OPSEC responsibilities for each site, facility, and program office whose name and contact information will be provided to the Office of Safeguards and Security Policy.
- Ensure OPSEC point of contact participation in the development of local implementation training and/or briefings tailored to the job duties of the individual employees.
- Develop and implement a comprehensive OPSEC awareness program that includes regular briefings to ensure that personnel are aware of their responsibilities in support of the OPSEC program. These briefings provide local implementation of national and Departmental requirements and may be integrated into, or provided in conjunction with, required security briefings (e.g., new hires' initial briefings, comprehensive or annual refresher briefings).
- Participate in self-assessments to ensure the national, Departmental, and local requirements to protect and control classified and unclassified controlled information are being followed in all areas and that employees are aware of their responsibilities.
- Provide information concerning deviations (e.g., variances, waivers, and exemptions) involving the OPSEC program to the Office of Safeguards and Security Policy and to the Associate Administrator for Defense Nuclear Security when involving NNSA facilities, in a timely fashion, to include implementation and expiration of such actions.
- Promulgate new OPSEC requirements to all affected employees.
- Interact and coordinate with the Office of Safeguards and Security Policy on OPSEC national and Departmental requirements interpretation and local implementation activities. Interaction and coordination between NNSA facilities and the Office of Safeguards and Security Policy is through the Associate Administrator for Defense Nuclear Security.

**b) Discuss the responsibilities of the OPSEC Manager.**

OPSEC plans must be developed for programs and operations and approved by the cognizant security authority.

**c) Discuss the activities, composition, and authorities of an OPSEC Working Group.**

Each organization should establish a sufficient number of OPSEC working groups to perform the necessary management and support functions required for an effective OPSEC program, to include OPSEC education and awareness. Working groups should develop and set priorities for their OPSEC program objectives consistent with approved plans and policies, meet on a regular basis, and maintain meeting records, a copy of which should be held by the responsible OPSEC manager.

**40. Safeguards and security personnel shall demonstrate a familiarity-level of knowledge of the classified computer security program as described in the following DOE directives:**

- **DOE O 471.2A, Information Security, Chapter III, Classified Information Systems Security**
- **DOE M 471.2-2, Classified Information Systems Security Manual**

Note: DOE O 471.2A, Information Security, has been cancelled. The information provided in this competency statement was taken from DOE M 471.2-2, Classified Information Security Systems Manual.

**a) Describe the types of automated information system security activities that are classified.**

All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, DOE on automated information systems requires some level of protection. The loss or compromise of information entrusted to DOE or its contractors may affect the nation's economic competitive position, the environment, the national security, DOE missions, or the citizens of the United States. The risk management approach defined for DOE and its contractors provides for the graded, cost-effective protection of automated information systems containing classified information.

**b) Discuss examples of classified automated information system security programs.**

Classified automated information systems (AISs) include but are not limited to the following examples:

- Mainframe Classified AISs, word processors, microprocessors, personal computers, programmable controllers, automated office support systems, memory typewriters, and other standalone or special systems that process, store, transfer, or provide access to classified information, including those classified AISs that also process, store, transfer, or provide concurrent or simultaneous access to classified and unclassified information
- Special purpose computers that perform classified functions and/or contain classified data, such as numerically controlled machines, smart switches, single-task preprogrammed controllers, programmable facsimile devices, automated testers, and digital to analog and analog to digital converters
- Networks wherein classified information is processed, stored, transferred, or accessed in one or more components of the network

**c) Identify and describe the classified automated information system security standards, policies, procedures, and objectives related to safeguards and security.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**41. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials.**

Note: DOE O 474.1, Control and Accountability of Nuclear Materials, and DOE M 474.1-1A, Manual for Control and Accountability of Nuclear Materials, have been cancelled. The information provided in this competency statement was taken from DOE M 470.4-6, Nuclear Material Control and Accountability.

**a) Discuss the basic requirements of material control and accountability.**

Nuclear material control and accountability programs must ensure accountable nuclear materials are accounted for and unauthorized acts are detected. These requirements must be applied in a manner consistent with the graded safeguards concept.

**b) Describe in general how the material control and accountability materials accounting systems provides a complete audit trail of all nuclear material from receipt through disposition.**

The accounting system must provide a complete audit trail for all nuclear material from receipt through disposition. The system tracks nuclear material inventories, documents nuclear material transactions, issues periodic reports, and assists with the detection of unauthorized system access, data falsification, and material gains or losses.

**c) Describe the general requirements of the material control and accountability physical inventory program for nuclear materials.**

*Conduct of Physical Inventories*

Inventories must be based on measured values, including measurements or technically justifiable estimates of holdup. Process monitoring techniques may be used for material that is undergoing processing and recovery operations and is inaccessible for measurements. Plans and procedures must be developed and documented to define responsibilities for performing inventories and specify criteria for conducting, verifying, and reconciling inventories. Statistical sampling, based on graded safeguards, may be used to verify the presence of items during inventories. Parameters for statistical sampling plans must be defined by the site/facility operator and approved by the DOE cognizant security authority. Sampling plans must specify the population, confidence level, minimum detectable defect, definition of a defect, and action to be taken if a defect is encountered.

*Physical Inventory Reconciliation Program*

A physical inventory reconciliation program must be implemented in which the book inventory for each MBA is compared with, and if necessary, adjusted to the physical inventory. The reconciliation must be completed within 15 calendar days following receipt of all inventory information, measurement data, and sample analyses. Any inventory differences must be identified and reported as required.

**d) Describe the general requirements and controls of the material control and accountability nuclear material transfer programs.**

*External Transfers*

The requirements for external transfers are as follows:

- The shipper must obtain written verification and maintain documentation that the intended receiver is authorized to accept the material before the material is transferred.
- Transfers of nuclear material between facilities having a different RIS must be documented using the electronic equivalent of DOE/NRC F 741. These forms must be prepared and distributed to the principals of the transaction and line management.
- Immediately after receipt, shipments must be subjected to a transfer check. Transfer checks must consist of confirming the shipping container or item count, validating the TID integrity and identification, verifying the tamper-indicating characteristics of the container, and comparing with shipping documentation to ensure the shipment was received intact.
- For all unirradiated Category I and II quantities of SNM transferred between facilities having a different RIS, the receiver must perform a verification or accountability measurement unless both RISs are located on the same site and are operated by the same site contractor.
- SNM in foreign reactor fuel returns must either be measured, or the risk of diversion of material from the fuel must be documented, and the acceptance of the fuel without measurement must be approved by the responsible Under Secretary or his/her designee.

*Internal Transfers*

The requirements for internal transfers are as follows:

- The site/facility operator must provide a graded system of measurements and records to reflect the flow of material between MBAs within that facility and between it and other facilities on the same site.
- The facility control system must be designed to monitor transfer activities and to deter and detect unauthorized removal of material during transfers. It must flag abnormal situations (e.g., inappropriate transfers of quantities or materials, or unauthorized personnel receiving or shipping materials).
- Transfers must be documented on nuclear material transfer forms or electronic equivalents that contain required information. They must be prepared and distributed within established time frames, and signed by authorized custodians or their alternates.
- Materials must be subjected to a transfer check within one work day after receipt. These checks must include verification of shipping container or item count, TID integrity (if applied), and identification number.
- When the isotope content of SNM transferred between MBAs is 50 grams (fissile) or more, the material must have a measured value before transfer.
- Acceptance/rejection criteria must be established and documented to evaluate measurement data for internal material transfers. In addition, procedures must specify notification and response requirements if nuclear material removal or another abnormal situation is detected.

**e) Discuss in general the four functional performance areas of nuclear material control.**

*Access Controls*

A graded program must be established to control personnel access to: nuclear materials; nuclear materials accountability, inventory, and measurement data; data-generating equipment; and other items/equipment, the misuse of which could compromise the safeguards system.

*Material Surveillance*

A nuclear materials surveillance program must ensure that nuclear materials are in their authorized locations, be capable of detecting unauthorized activities or anomalous conditions, and be capable of reporting material status. The surveillance program must address both normal and emergency conditions and include periodic testing.

*Material Containment*

A documented program must be in place to provide controls for nuclear materials operations relative to MAAs, PAs, MBAs, other authorized storage repositories, and processing areas.

*Detection/Assessment*

Systems must be in place to detect and assess the unauthorized removal of nuclear materials, consistent with the graded safeguards concept. The system must be interfaced with the facility's physical protection and other organizational systems, as appropriate, and must be able to detect and localize removal of SNM from its authorized location, and notify the PF and other organizations to respond when such events are detected.

**42. Safeguards and security personnel shall demonstrate a working-level knowledge of DOE M 475.1-1A, Identifying Classified Information.**

**a) Discuss the responsibilities of field elements and contractor employees in identifying classified information.**

Heads of program and support offices within DOE, including NNSA, must ensure that information, documents, and material are reviewed and processed in accordance with requirements in DOE M 475.1-1A.

Heads of DOE elements, NNSA Deputy Administrators, and managers of field elements must

- ensure that the necessary staff are designated to fulfill the requirements contained in DOE M475.1-1A;
- ensure that information, documents, and material are reviewed and processed in accordance with the requirements in DOE M 475.1-1A;
- ensure that Headquarters classification representatives, classification officers, and other personnel with classification responsibilities participate in the early planning stages of any new program that may generate classified information, documents, or material;
- ensure that the management of classified information is included as a critical element or item to be evaluated in the performance standards of Headquarters classification representatives, classification officers, original classifiers, and any other individuals whose duties include significant involvement in generating classified information, documents, or material;

- identify/appoint an individual to be responsible for notifying the contracting officer of each procurement falling within the scope of DOE M 475.1-1A. (If such an individual is not identified or appointed, the person originating the procurement request assumes this responsibility.)

Headquarters classification representatives
- serve as the points of contact with the Office of Nuclear and National Security Information for their Headquarters elements;
- coordinate the classification and declassification reviews of documents and material for their organizations;
- assist individuals within their organizations in implementing the classification and declassification policies and procedures in DOE M 475.1-1A, and refer questions, as necessary, to the Office of Nuclear and National Security Information.

Field element classification officers
- serve as the points of contact with the Office of Nuclear and National Security Information for their field elements;
- administer the field element classification and declassification programs;
- ensure that a classification review is performed prior to the dissemination of each document that may be classified, and that is prepared by a field element employee.

**b) Discuss the general policies and objectives of the DOE classification program.**

The Office of Nuclear and National Security Information manages the classification and declassification oversight program that ensures that all DOE, including NNSA, and their contractor and subcontractor organizations that generate classified information and documents or material have implemented and maintain an adequate and effective classification and declassification program.

**c) Discuss the criteria for classification.**

Classification is determined by the classification guidance. At a minimum, classification guidance identifies elements of information that are classified or unclassified in a specific area. For classified information, the guidance prescribes the classification level and category. For information classified as NSI, the guidance also states a concise reason for classifying the information and prescribes declassification instructions or the category for exemption from automatic declassification for each element of information.

**d) Describe the classification levels, use of the terms unclassified, and mosaic compilation.**

*Levels of Classification*

The following levels of classification, listed in descending order of sensitivity, may be applied to RD, FRD, or NSI:
- Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.

- Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- Confidential. The damage tests for RD/FRD and NSI are different, as noted below:
  - RD/FRD. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - NSI. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.

*Categories of Classified Information*

RD is information classified under the Atomic Energy Act that concerns

- the design, manufacture, or utilization of nuclear weapons;
- the production of special nuclear material;
- the use of SNM in the production of energy.

RD does not include information declassified or removed from the RD category under Section 142 of the Atomic Energy Act.

FRD is information classified under the Atomic Energy Act that relates primarily to the military utilization of nuclear weapons and that has been removed from the RD category by a joint determination between DOE and the Department of Defense.

NSI is information that has been determined under Executive Order 12958 or any predecessor Executive orders to require protection against unauthorized disclosure and that is marked to indicate its classified status when contained in a document.

*Unclassified*

The term "Unclassified" is used to identify information that is not classified under a statute or Executive order. Unclassified information is not normally marked as "Unclassified" except to distinguish it from classified information, and then only when such distinction is required or otherwise serves a useful purpose. The fact that information is unclassified does not mean that it may be released to the public.

**e) Discuss the availability of site classification guidance.**

Local guidance has the same purpose as Headquarters guidance, but is more detailed and is tailored to the specific needs of the originating field element or contractor organization. If existing Headquarters guidance is adequate for the needs of the organization, local guidance is not required. If proposed local guidance affects DOE, including NNSA, elements other than the issuing organization, a Government agency other than DOE (such as the Department of Defense), or a foreign government, the Director of Nuclear and National Security Information shall issue Headquarters guidance to cover the information.

**f) Describe the classification/security markings placed on a classified document.**

*General Requirements*

Classified matter, regardless of date or agency of origin, must be marked to indicate at least the classification level and category (if RD or FRD). Documents must be marked in accordance with directives in place at the time of origin or later, or in accordance with current directives. If there is a question about the classification level or category of a document, the document must be reviewed by a derivative classifier and re-marked (if necessary) to clearly indicate the level and category and to ensure proper protection. When possible, avoid returning documents because of improper markings. Instead, contact the sender and attempt to resolve any marking issues.

Classified NSI documents that were created after April 1, 1996, and that lack appropriate current markings, including declassification on a date or event, classification authority, or classifier's name, should be reviewed by a derivative classifier to ensure the classification level and category are still correct, and then re-marked to bring them into conformance with current marking requirements. This must be done if the document is active or is to be transmitted outside of the organization for other than official archiving purposes. Documents created before April 1, 1996, need only contain classification level and category (if RD or FRD) to ensure proper protection.

*Markings*

The following elements are common to all classified documents: classification level, classification category (if RD or FRD), caveats and/or special markings (if required), classifier information, originator identification, classification of titles or subjects, unique identification numbers (if in accountability), and portion marking (if NSI). The DOE Marking Handbook provides guidance and examples for marking classified documents. The originator is responsible for ensuring that each classified document is marked correctly.

*Unique Identification Numbers*

Classified matter required to be in accountability must have a unique identification number. To ensure control and accountability of this matter, the unique identification number must be placed on the first page of paper documents and on the top or front of non-paper documents. The first page of a document is the first sheet of paper (i.e., the cover page, title page, or first page of text).

*Originating Organization and Date*

The name of the organization responsible for preparing the document and the date of preparation must appear on the first page of all classified documents. The first page of a document is the first sheet of paper, whether that is the cover page, title page, or first page of text. Classified documents being taken offsite must be marked on the first page to show the mailing address of the organization responsible for preparing the document. The mailing address should consist of a street address or post office box, city, state, and zip code. Note: When information cannot be accommodated on the first page, such as in the case of slides, microfiche, etc., this information must conspicuously accompany the classified document on a separate piece of paper.

*Classification Level*

The three classification levels, in descending order of sensitivity and potential damage to the National security, are Top Secret, Secret, and Confidential. Requirements for marking documents and materials are listed below:

- The overall classification level (i.e., Top Secret, Secret, or Confidential) of a document must be marked on the top and bottom of the cover page (if any), the title page (if any), the first page of text, and the outside of the back cover or last page of text.
- Each interior page of a classified document must be marked top and bottom with the highest classification level (or marked unclassified, if applicable) of that page or the overall classification of the document.
- Classification markings must be clearly distinguishable from the document text.
- Classified material must have the classification level stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.
- Blank interior pages of a classified document need not be marked with the classification level or category or the notice "This page intentionally left blank."

*Classification Categories*

The three classification categories are RD, FRD, and NSI. Classified documents containing only NSI need not be marked with the NSI category marking. If the document is RD or FRD, the appropriate admonishment information must be marked on the first page of the document, whether that be the cover page, title page, or first page of text, and should appear in the lower left corner, as follows:

RESTRICTED DATA
This document contains Restricted Data as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.

FORMERLY RESTRICTED DATA
Unauthorized disclosure is subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination per Section 144.b, Atomic Energy Act, 1954.

Each interior page of a document containing RD or FRD must be marked top and bottom with the appropriate level and category of information on that page. If this is not feasible, the overall level and category of the document (if RD or FRD) may be applied to every page. For interior pages, the symbols RD and FRD may be used. These markings must be clearly distinguishable from the document text.

Classified material (if RD or FRD) must have the classification category stamped, printed, etched, written, engraved, painted, or affixed to it by means of a tag, sticker, decal, or similar device. When marking is not practical, written notification of the markings must be furnished to recipients.

*Portions*

For NSI documents, each section, part, paragraph, graphic, figure, or similar portion of any such document dated after April 1, 1997, must be marked to show the classification level or

be identified as unclassified controlled information (e.g., UCNI, OUO) or as unclassified (U). Classification levels of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion.

Documents containing RD or FRD are not required to be portion marked; however, in cases where portion markings are used, classification levels and categories (if RD or FRD) of portions of a document must be shown by placing the appropriate classification symbol immediately following the portion's letter or number, or in the absence of letters or numbers, immediately before the beginning of the portion. Each section, part, paragraph graphic, figure, or similar portion of any such document must be accurately marked to show

- the classification level and category (e.g., SRD or S/RD, CFRD or C/FRD, S, TS)
- that it is unclassified controlled information (e.g., UCNI, OUO)
- that it is unclassified (U)

Portion markings must include any applicable caveats.

*Subjects and Titles*

Except for extraordinary circumstances, unclassified subject descriptors and titles must be used for classified documents because they are used on mail logs, document receipts, and other tracking or accountability records, most of which are entered into unclassified databases. Titles of classified documents must be marked, even if the document is not portion marked. The classification or control symbols (e.g., U, OUO, UCNI, C/RD, S/FRD) must be placed immediately after the title or subject.

When classified documents with unmarked titles and/or subjects become active (i.e., are sent outside the office of origin or holder, or are removed from storage), the titles and/or subjects of the classified documents must be reviewed by a derivative classifier and marked appropriately.

*Authorized Markings for Portions, Subjects, and Titles*

The following are examples of the markings authorized for use with subjects and titles and when portion marking:

Unclassified: (U)
Official Use Only: (OUO)
Unclassified Controlled Nuclear Information: (UCNI)
Confidential National Security Information: (C)
Confidential Formerly Restricted Data: (C/FRD) or (CFRD)
Confidential Restricted Data: (C/RD) or (CRD)
Secret National Security Information: (S)
Secret Formerly Restricted Data: (S/FRD) or (SFRD)
Secret Restricted Data: (S/RD) or (SRD)
Top Secret National Security Information: (TS)
Top Secret Restricted Data: (TS/RD) or (TSRD)
Top Secret Formerly Restricted Data: (TS/FRD) or (TSFRD)

**43. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the requirements for control of Top Secret, Secret, and Confidential documents as described in the DOE directives listed below:**

- **DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests**
- **DOE M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests**

Note: DOE Order 5632.1C, Protection and Control of Safeguards and Security Interests, and DOE M 5632.1C-1, Manual for Protection and Control of Safeguards and Security Interests, have been cancelled. The information provided in this competency statement was taken from DOE M 475.1-1A, Identifying Classified Information.

**a) Discuss classification levels and the degree of control required for each of the above directives.**

The three classification levels, in descending order of sensitivity and potential damage to national security, are Top Secret, Secret, and Confidential:

- Top Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security in a way that the appropriate official can identify or describe.
- Secret. This level is applied to information whose unauthorized disclosure could reasonably be expected to seriously damage the national security in a way that the appropriate official can identify or describe.
- Confidential. The damage tests for RD/FRD and NSI are different, as noted below:
  - RD/FRD. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to cause undue risk to the common defense and security in a way that the appropriate official can identify or describe.
  - NSI. This confidential level is applied to information whose unauthorized disclosure could reasonably be expected to damage the national security in a way that the appropriate official can identify or describe.

**b) Describe the appropriate clearance level for access to each classification level.**

In accordance with the Atomic Energy Act:

| Access Level | RD | FRD | NSI |
|---|---|---|---|
| Q | TS, S, C | TS, S, C | TS, S, C |
| L | C | S, C | S, C |

Legend:
RD= Restricted Data, FRD= Formerly Restricted Data, NSI= National Security Information
TS= Top Secret, S= Secret, C= Confidential

**44. Safeguards and security personnel shall demonstrate a working-level knowledge of DOE O 471.2A, Information Security Program.**

Note: DOE O 471.2A, Information Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, and DOE M 471.2-2, Classified Information Security Systems Manual.

**a) Discuss the purpose and policy statements associated with the DOE's information security program.**

DOE M 471.2-2 provides requirements and implementation instructions for the graded protection of the confidentiality, integrity, and availability of information processed on all automated information systems used to collect, create, process, transmit, store, and disseminate classified information by, or on behalf of, DOE. The requirements are based upon applicable federal statutes, regulations, National Security Directives, Executive orders, procedures in Office of Management and Budget (OMB) circulars and bulletins, and federal standards.

All information collected, created, processed, transmitted, stored, or disseminated by, or on behalf of, DOE on automated information systems requires some level of protection. The loss or compromise of information entrusted to DOE or its contractors may affect the nation's economic competitive position, the environment, the national security, DOE missions, or the citizens of the United States. The risk management approach defined for DOE and its contractors provides for the graded, cost-effective protection of automated information systems containing classified information.

**b) Describe the major elements of the information security program.**

The three main elements of the information security program are management structure, risk management, and requirements.

*Management Structure*

Management of the Classified Information Systems Security Program is performed through a multi-tiered structure. DOE positions include the Classified Information Systems Security Program Manager (ISPM), Designated Approving Authority(s) (DAA), and Classified Information Systems Security Operations Manager(s) (ISOM). Site positions, which may be held by DOE or contractor employees, include Classified Information Systems Security Site Manager(s) (ISSMs) and Classified Information Systems Security Officer(s) (ISSO). Site positions also include application owners/data custodians and users.

*Risk Management*

Risk management is a process that considers the prevailing DOE threat analysis, the effect of countermeasures applied to the processing environment, the remaining vulnerability of the processing environment (residual risk), and the protection requirements and value of the information being processed. Countermeasures are increased until the risk is reduced to an acceptable level, or until the cost of reducing the risk becomes prohibitive. If the DAA determines that the remaining risk is not acceptable, management must then determine if the automation requirements are sufficient to justify additional costs.

*Requirements*

The Department's classified information systems security process for achieving adequate protection is based on levels of concern for the confidentiality, integrity, and availability of information. Requirements common to all systems include sanitization, maintenance, personnel, and physical requirements. Protection requirements are graded by levels of concern and confidentiality protection level, and include audit, documentation, and testing requirements.

**c) Discuss the duties and responsibilities of the following positions as they pertain to the information security program:**
- **Heads of departmental elements**
- **Heads of field organization**
- **Information security program operations managers**
- **Procurement request originators**
- **Contracting officers**

The Classified Information Systems Security Program is managed through a multi-tiered structure. The structure includes an ISPM at DOE Headquarters, DAA(s), ISOM(s) at each DOE Operations Office, and ISSMs and ISSOs at the sites. The structure also includes application owners/data custodians and users of the systems.

*Classified Information Systems Security Program Manager (ISPM)*

The ISPM is a DOE employee knowledgeable in information systems security and appointed by the Director of the Office of Safeguards and Security (NN-51). The ISPM
- serves as the program manager for Classified Information Systems Security and ensures implementation of the Classified Information Systems Security Program within DOE;
- develops and recommends DOE policies, standards, procedures, and guidelines for protecting information systems that collect, create, process, transfer, store, or provide access to classified information;
- maintains a continuing review of DOE M 471.2-2 to ensure that current technology is being applied to the protection of information systems that create, process, store, transfer, or provide access to classified information, and to eliminate those practices that are no longer needed or effective;
- approves secure remote diagnostic and maintenance facilities proposed for use with information systems that process classified information;
- annually reviews and updates, as needed, the Periodic Risk Assessment for the DOE Classified Information Systems Security Program and the DOE Statement of Generic Threat to Automated Information Systems;
- in coordination with the field, designates the DAA for information systems that operate under the jurisdiction of more than one Headquarters and field element;
- reviews and concurs on accreditation for systems operating at Protection Level 5 or 6 that operate under the jurisdiction of one Headquarters or field element;
- represents the DOE before federal, private, and public organizations concerned with protecting classified information systems;
- reports changes in ISOM and DAA appointments to all DAAs;
- Coordinates
  - with the Unclassified Computer Security Program Manager;

    - with the Office of Energy Intelligence on the protection of Sensitive Compartmented Information (SCI);
    - implementation of the Classified Information Systems Security Program with Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, MC&A, and other programs, as appropriate;
    - the development, publication, and distribution of guidelines for the protection of classified information systems;
- provides education, awareness, and training activities that
    - ensure that education in DOE's Classified Information Systems Security Program policies and practices is available to the ISOMs and ISSMs (scheduling of these educational activities must allow all ISOMs and ISSMs to participate within one year of their appointment);
    - maintain a capability to facilitate the electronic exchange of information systems security information, such as awareness alerts on sniffer attacks, viruses, etc.;
    - periodically present information systems security workshops;
    - periodically sponsor an Information Systems Security Program training conference;
- supports, maintains, and coordinates an advice and assistance capability for use by any ISOM or ISSM within DOE, with the services provided by this capability to include
    - advice and assistance reviews of information systems protection as requested by the site, such as reviews of network designs or protection profiles of networks or systems;
    - independent validation and verification (IV&V), such as design, certification, and performance test reviews of networks or systems that process classified information;
- maintains and coordinates an incident response capability to provide timely assistance and system vulnerability information to DOE sites;
- provides guidance for a technology development program to support the Classified Information Systems Security Program, and periodically briefs DAAs, ISOMs, and ISSMs on activities and results of the program;
- collects and disseminates information relevant to the Classified Information Systems Security Program;
- monitors the Classified Information Systems Security Program findings and deficiencies resulting from surveys, inspections, and reviews;
- conducts timely reviews of the system protection documentation and the certification for information systems located in Sensitive Compartmented Information Facilities (SCIFs) received from cognizant ISOMs, and provides comments to the Office of Energy Intelligence.

*Designated Approving Authority (DAA)*

The DAA is a DOE employee appointed by the Operations Office Manager. He/she is responsible for evaluating the protection measures in an information system as described in the Classified Information Systems Security Plan (ISSP), the results of any certification tests, the certification of the system, and any residual risks of operating the system. The DAA may designate additional tests that must be performed prior to meeting accreditation requirements.

With this appointment, the operations manager provides the DAA with written authorization to accept the residual risks and responsibility for the loss of confidentiality, availability, and/or integrity of all classified information systems under DAA jurisdiction. The authorization must include accreditation, provisional accreditation, withdrawal of accreditation, and suspension of operations for all classified information systems with operational boundaries fully contained under his/her jurisdiction. The ISOM may also be appointed as the DAA. The DAA

- serves as accrediting authority for each DOE and covered contractor classified information system with operational boundaries fully contained under his/her jurisdiction;
- ensures that DOE M 471.2-2 is implemented for each classified information system under his/her jurisdiction, that each system is accredited or reaccredited every three years (except for information systems that process SCI), and that the accreditation or reaccreditation is documented;
- ensures that the accreditation of each system under his/her jurisdiction is withdrawn, and that the system is properly sanitized when the system no longer processes classified information or when changes occur that might affect accreditation;
- ensures that DAA authorities are delegated only to DOE employees who are knowledgeable in information systems security;
- reports any changes in ISOM or ISSM appointments to the ISPM.

*Classified Information Systems Security Operations Manager(s) (ISOM)*

The ISOM is a DOE employee that is knowledgeable in information systems security and appointed by the operations office manager. The ISOM must participate in ISPM-sponsored training in the Classified Information Systems Security Program within one year of his/her appointment. The ISOM

- communicates appropriate incident reports received from sites to the ISPM;
- ensures periodic review of the Classified Information Systems Security Program consistent with the Operations Office Survey Program at each site under the jurisdiction of the DOE operations office;
- evaluates information systems for accreditation and provides results to the DAA;
- monitors responses to findings and other deficiencies identified in surveys, inspections, and reviews of each site's Classified Information Systems Security Program to ensure that any necessary corrective or compensatory actions have been completed;
- coordinates
  - the Classified Information Systems Security Program with the Unclassified Information Systems Security Program;
  - implementation of the Classified Information Systems Security Program with requirements of other DOE programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and MC&A programs.

*Classified Information Systems Security Site Manager(s) (ISSM)*

The ISSM is appointed by the site manager to be responsible for implementation of the site Classified Information Systems Security Program. A separate ISSM may be appointed for information systems in an SCIF if the site determines that another ISSM is needed. In this

capacity, the ISSM also functions as the site point of contact (POC) for all classified information systems security issues. The ISSM

- ensures the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users which must include, but is not limited to, various combinations of self-paced and formal classes, security education bulletins, training films, computer-aided instruction, security briefings, and related educational aids;
- ensures the development, documentation, and presentation of information systems security training for escorts in information systems operational areas;
- establishes, documents, implements, and monitors the Classified Information Systems Security Program for the site, and ensures site compliance with DOE requirements for information systems;
- ensures the development of procedures for use in the site Classified Information Systems Security Program;
- identifies and documents unique threats to information systems at the site;
- ensures that the site's Classified Information Systems Security Program is coordinated with the SSSP or the SSP;
- coordinates
  - implementation of the site Classified Information Systems Security Program with the other site programs, as appropriate, such as Classified Matter Protection and Control, Personnel Security, Physical Security, Communications Security, Protected Transmission Systems, TEMPEST, and MC&A;
  - development of a site self-assessment program for the Classified Information Systems Security Program;
  - self-assessment of the site's Classified Information Systems Security Program, which is to be performed between operations office surveys;
- ensures the development of site procedures to
  - govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;
  - ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;
  - report classified information systems security incidents;
  - require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for the security of classified information systems and classified information;
  - detect malicious code, viruses, and intruders (hackers);
  - review and approve ISSPs, certification test plans, and certification test results.
- determines, using guidance from the data custodian(s), the appropriate levels of concern for confidentiality, integrity, and availability for each information system that processes classified information;
- certifies to the DAA, in writing, that each ISSP has been implemented, that the specified protection measures are in place and properly tested, and that the classified information system is functioning as described in the ISSP;
- recommends to the DAA, in writing, approval or disapproval of the ISSP test results and the certification statement;

- ensures that the DAA is notified when a system no longer processes classified information or when changes occur that might affect accreditation;
- participates in ISPM-sponsored information systems security training within one year of his/her appointment;
- ensures that personnel are trained on the information system's prescribed security restrictions and safeguards before they are initially allowed to access a system.

*Classified Information Systems Security Officer(s) (ISSO)*

The ISSO

- ensures implementation of security measures for each classified information system for which he/she is responsible;
- identifies and documents any unique threats to classified information systems for which he/she is the ISSO and forwards them to the ISSM;
- if so directed by the DAA and/or if an identified unique local threat exists, performs a risk assessment to determine if additional countermeasures are required;
- develops and implements a certification test plan for each classified information system for which he/she is the ISSO;
- prepares, maintains, and implements an ISSP that accurately reflects the installation of protection measures for each classified information system for which he/she is responsible;
- maintains the record copy of the ISSP and related documentation for each classified information system for which he/she is the ISSO;
- notifies the DAA (through the ISSM) when a system no longer processes classified information, or when changes occur that might affect accreditation;
- ensures that
  - the sensitivity level of the information is determined prior to use on the classified information system and the proper security measures are implemented to protect this information;
  - unauthorized personnel are not granted use of, or access to, a classified information system;
  - formal access controls are implemented for each classified information system, except stand-alone personal computers and stand-alone workstations;
- documents any special protection requirements identified by the data custodians and the protection measures implemented to fulfill these requirements for the information contained in the classified information system;
- ensures that confidentiality, integrity, and availability levels of concern are determined for each classified information system for which he/she is responsible;
- implements site procedures to
  - govern marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media and equipment containing classified information;
  - ensure that vendor-supplied authentication features (e.g., passwords, account names) or security-relevant features are properly implemented;
  - report classified information systems security incidents;
  - require that each classified information system user sign an acknowledgment of responsibility (Code of Conduct) for protecting classified information systems and classified information;
  - detect malicious code, viruses, and intruders (hackers);
  - review and approve ISSPs, certification test plans, and certification test results;

- ensures that users are properly trained in system security by identifying classified information systems security training needs (including system-specific training) and personnel who need to attend system security training programs;
- conducts ongoing security reviews and tests of classified information systems to periodically verify that security features and operating controls are functional and effective;
- evaluates proposed changes or additions to the classified information systems and advises the ISSM of their security relevance.

**d) Describe the facility's chain of responsibility for information security.**

The following are in addition to the responsibilities given in element "c."

*Classified Information Systems Application Owner/Data Custodian*

The application owner/data custodian

- determines and declares the sensitivity level of information prior to the information being processed, stored, transferred, or accessed on the classified information system;
- advises the ISSO of any special protection requirements for information to be processed on the classified information system;
- determines and documents the data and application(s) that are essential to fulfill the site mission, and ensures that requirements for contingencies are determined, implemented, and tested;
- ensures that information is processed on a classified information system that is accredited at a level sufficient to protect the information.

*Users of Classified Information Systems*

Users of classified information systems must

- comply with the Classified Information Systems Security Program requirements;
- be aware of and knowledgeable about their responsibilities in regard to classified information systems security;
- be accountable for their actions on a classified information system;
- ensure that any authentication mechanisms (including passwords) issued for the control of their access to classified information systems are not shared and are protected at the highest classification level and most restrictive classification category of information to which they permit access;
- acknowledge, in writing, their responsibilities (Code of Conduct) for protecting classified information systems and classified information;
- participate in training on the information system's prescribed security restrictions and safeguards before receiving initial access to a system, and as a follow-up to this initial training, participate in an ongoing security education, training, and awareness program.

**e) Discuss the facility's security organization program guidelines.**

This is a site-specific competency. The qualifying official will evaluate the completion of this competency.

**f) Describe the process of dealing with classified matter that cannot be accounted for.**

Incidents of security concern are actions, inactions, or events that have occurred at a site that

- pose threats to national security interests and/or critical DOE assets
- create potentially serious or dangerous security situations
- potentially endanger the health and safety of the workforce or public (excluding safety-related items)
- degrade the effectiveness of the S&S program
- adversely impact the ability of organizations to protect DOE S&S interests

Incidents of security concern must be categorized in accordance with their potential to cause serious damage or place S&S interests and activities at risk. Four categories of security incidents have been established based on the relative severity of the incident. Each of the four categories is identified by an IMI number as follows (from most severe to least severe): IMI-1, IMI-2, IMI-3, and IMI-4. Each of the four categories is further subdivided into specific subcategories based on the security topical areas of physical protection, PF, information security, personnel security, and nuclear MC&A. The categorization of specific security incidents occurs at the time the security incident is discovered. The categorization of specific security incidents can change based on information developed during the inquiry into the incident.

*Reporting Requirements*

The 24-Hour Determination/Categorization Period. When an incident is suspected to have occurred, the cognizant security authority at the site/facility where the incident occurred has 24 hours to examine and document all pertinent facts and circumstances to determine whether an incident has occurred. During this period, the suspected incident must be categorized by an IMI number. If it is determined that an incident of security concern did not occur, no further action is required.

Initial Incident Reporting. Incidents of security concern initial reports for IMI-1, IMI-2, and IMI-3 (as well as those for IMI-4 involving non-U.S. citizens) must be sent to the DOE HQ OC using DOE Form (F) 471.1, Security Incident Notification Report, in accordance with locally developed procedures approved by line management. Initial security incident reports must be forwarded based on the following criteria:

- Within one hour following categorization for security incidents determined to be IMI-1, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.
- Within eight hours following categorization of security incidents determined to be IMI-2/IMI-3, the cognizant security authority at the originating site/facility must transmit a DOE F 471.1 to the DOE HQ OC. If a verbal notification of the incident is made to the DOE HQ OC, a follow-up transmission of the DOE F 471.1 to the DOE HQ OC must still be made.

Reporting Incidents Receiving Media Attention. In addition to the IMI reporting time frames, the Office of Security must be notified within eight hours of any security incidents that have been or will be reported in the media. The initial DOE F 471.1 and any subsequent updates must clearly identify the fact of media reporting.

Reporting Incidents Associated with Non-U.S. Citizens. Security incidents having any association with non-U.S. citizens must be clearly identified and reported on the initial DOE F 471.1, and subsequently in any related update or follow-on activity pertaining to the incident, including incidents categorized as IMI-4. For security incidents involving any credible information that a non-U.S. citizen or an agent of a foreign power is involved, the geographically closest element of the OCI/ODNCI must be notified.

Numbering Incidents and Changing Categories. When the initial incident notification report (i.e., DOE F 471.1) is transmitted, it must include a local incident tracking number. All subsequent reports pertaining to a security incident (e.g., inquiry and other related activities) must be transmitted to the Office of Security. Changes in IMI categorizations require resubmission of a DOE F 471.1 (or form similar in content) to the Office of Security.

Reporting Incidents Associated with Sensitive Programs. Only the initial DOE F 471.1 is required for incidents involving activities associated with sensitive programs. These programs include the SCI Program, the SAP, the TSCM Program, the CI Program, or other programs identified by the Office of Security. All subsequent reporting must be handled "within channels" until such time as the inquiry report has been distributed. The date of the inquiry report must be transmitted to the Office of Security for entry into the Incident Tracking and Analysis Capability database.

Inquiries are considered closed under the following conditions:

- IMI-1 and IMI-2 incidents are considered closed upon completion of the inquiry report. The inquiry report must be completed within 60 working days of the incident categorization or a status report must be provided.
- IMI-3 incidents are considered closed upon completion of DOE F 5639.3, Report of Security Incident/Infraction, and transmission of the completed DOE F 5639.3 to the Office of Security. The completion of the section on assignment and acceptance of security infractions (Part II, DOE F 5639.3) must be completed as required in local procedures.
- IMI-4 incidents are considered closed upon completion of the DOE F 5639.3 in accordance with associated local procedures.

A sanitized (unclassified) copy of the DOE F 5639.3 must be provided to the responsible personnel security office for placement in the appropriate personnel security file.

*Final Inquiry Reports*

Inquiry officials must forward final inquiry reports in accordance with local procedures to line management for action and to the Office of Security.

*Inquiry Officials*

Requirements for inquiry officials are as follows:

- Inquiry officials must conduct inquiries to establish the pertinent facts and circumstances surrounding incidents of security concern.
- Inquiry officials may be either federal or contractor employees, but must have previous investigative experience or Department inquiry training, and must be knowledgeable of appropriate laws, Executive orders, Departmental directives, and/or regulatory requirements.

- Inquiry officials are not authorized to detain individuals for interviews or to obtain sworn statements; however, they may conduct consensual interviews and obtain signed statements.
- Inquiry officials must be appointed in writing by the DOE line management, the head of the Office of Headquarters Security Operations, or the Office of Security.
- Inquiry officials are responsible for conducting the inquiry and maintaining records and documentation associated with the inquiry (e.g., logs of events, notes, recordings, and statements).
- When inquiry officials discover suspected or confirmed violations of law, they must immediately notify the Office of Security.

*Conduct of Inquiries*

If an incident affects more than one site/facility, the following criteria must be used in determining the lead organization responsible for conducting the inquiry:

- If the sites/facilities fall under the purview of a single DOE cognizant security authority, that DOE cognizant security authority must assign responsibility to a lead organization.
- If the sites/facilities fall under the purview of multiple DOE cognizant security authorities, those DOE cognizant security authorities must, by mutual agreement, decide on a lead organization with responsibility for the inquiry.

The following actions must be taken when conducting inquiries into incidents of security concern and be reflected in the inquiry report:

- Data Collection.
  - Collect all data/information relevant to the incident, such as operations logs, inventory reports, requisitions, receipts, photographs, signed statements, etc.
  - Conduct interviews to obtain additional information regarding the incident.
  - Collect physical evidence associated with the inquiry, if available. (Examples of physical evidence include, but are not limited to, recorder charts, computer hard drives, defective/failed equipment, procedures, readouts from monitoring equipment, etc.)
  - Ensure physical evidence is protected and controlled and a chain of custody is maintained.
- Incident Reconstruction.
  - Reconstruct the incident of security concern to the greatest extent possible using collected information and other evidence.
  - Develop a chronological sequence of events that describes the actions preceding and following the incident.
  - Identify persons associated with the incident.
- Incident Analysis and Evaluation.
  This analysis determines which systems/functions performed correctly or failed to perform as designed. It provides the basis for determining the cause of the incident and subsequent corrective actions. Inquiry officials must perform the following tasks:
  - Analyze the information collected during the inquiry to determine whether it describes the incident completely and accurately.
  - Collect additional data and reconstruct the incident if more information is required.
  - Identify any collateral impact with other programs or security interests.

In addition, inquiry officials must perform the following actions:

- Interview custodians and others having knowledge of the incident. When necessary, records must be audited for evidence of destruction, transmission, or other disposition.
- Ensure a DOE F 5639.2, Reporting Unaccounted for Documents, or a form comparable in content, is completed if classified information or matter is missing.
- Determine which Departmental element has programmatic responsibility for the information or whether the information was originated by another Government agency or foreign government.
- Determine whether a compromise or potential compromise occurred. If there was a potential compromise, seek to determine the probability of compromise. Document the basis for such findings (i.e., potential compromise is defined as an incident of security concern where circumstances exist that cannot rule out the compromise of classified information).
- If an inquiry determines that a compromise or potential compromise has occurred, document the extent of the dissemination of the classified information and the actions taken to prevent further dissemination.
- When an inquiry establishes that classified information has been compromised by being published in the media, the questions contained in the DOJ Eleven-Point Criteria, which are listed below, must be answered and coordinated with the Office of Security. When completing the questions, provide all documentation and appropriate information to support affirmative responses. Each question must be answered affirmatively before the DOJ will initiate a formal investigation into the compromise; however, failure to affirmatively answer all the DOJ criteria does not preclude the DOJ from pursuing administrative or criminal action.
  - Could the date and identity of the article or articles disclosing the classified information be provided?
  - Could specific statements in the article that are considered classified be identified? Was the data properly classified?
  - Is the classified data that was disclosed accurate? If so, provide the name of the person competent to testify concerning the accuracy.
  - Did the data come from a specific document, and, if so, what is the origin of the document and the name of the individual(s) responsible for the security of the classified data disclosed?
  - Could the extent and official dissemination of the data be determined?
  - Has it been determined that the data has not been officially released in the past?
  - Has it been determined that prior clearance for publication or release of the information was not granted by proper authorities?
  - Does review reveal that educated speculation on the matter cannot be made from material, background data, or portions thereof which have been published officially or have previously appeared in the press?
  - Could the data be made available for the purpose of prosecution? If so, include the name of the person competent to testify concerning the classification.
  - Has it been determined that declassification had not been accomplished prior to the publication or release of the data?
  - Will disclosure of the classified data have an adverse impact on the national defense?

**g) Describe the process of dealing with the compromise of classified matter.**

See information in element "f" of this competency statement.

**h) Describe the process of making a damage assessment.**

*Conduct of Damage Assessments*

The Departmental element with programmatic responsibility for the compromised or potentially compromised classified information must designate, in writing, a federal employee from the DOE cognizant security authority who will be responsible for conducting the damage assessment. The Departmental element must also appoint an assessment team consisting of a derivative classifier and appropriate technical experts (e.g., experts in weapons design, nuclear policy, material production communications, intelligence, counterintelligence) to assist in assessing the value of the compromised information to foreign governments and/or hostile organizations and the impact on the affected program.

*Procedures*

The following damage assessment procedures must be followed:

- The originator of the compromised information must provide the DOE cognizant security authority with a copy of the compromised or potentially compromised information, if available. If no other copy exists, the originator must provide a detailed description of the compromised information.
- The originator must coordinate with a derivative classifier to confirm the classification level and category of the compromised information according to current classification guidance and policy. The derivative classifier must provide the basis for the classification determination (i.e., the classification guide used).
- The team performing the damage assessment must prepare a draft assessment and coordinate it with the originator of the compromised or potentially compromised information.
- The damage assessment must be approved by the Departmental element with programmatic responsibility for the compromised or potentially compromised information, and at a minimum, copies will be submitted to the Director, Office of Security, and the DOE cognizant security authority responsible for the inquiry.
- The Director, Office of Security, will coordinate with the Departmental element and distribute additional copies as appropriate.

**i) Describe the process of determining, assigning, and reporting a security infraction of classified information.**

Whenever possible, the responsibility for an incident of security concern must be assigned to an individual rather than to a position or office.

When individual responsibility cannot be established and the facts show that a responsible official allowed conditions to exist that led to an incident of security concern, responsibility must be assigned to that official.

Security infractions are issued to document the assignment of responsibility for an incident of security concern. Individuals who do not possess an access authorization may be issued a security infraction.

**45. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of DOE O 470.1, Safeguards and Security Program.**

Note: DOE O 470.1, Safeguards and Security Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management, DOE M 470.4-7, Safeguards and Security Program References, and DOE O 470.4, Safeguards and Security Program.

**a) Discuss the policy set forth in this order.**

DOE O 470.1, Safeguards and Security Program, has been cancelled.

**b) Describe the purpose of safeguards and discuss the types of activities used to accomplish these purposes.**

The DOE S&S Program consists of six key elements: 1) Program Planning and Management, 2) Physical Protection, 3) PF, 4) Information Security, 5) Personnel Security, and 6) Nuclear Material Control and Accountability. Specific requirements for each of the key elements are contained in their respective programmatic Manuals. The requirements identified in these Manuals are based on national level policy promulgated in laws, regulations, and Executive orders, to prevent unacceptable adverse impacts on national security, the health and safety of DOE and contractor employees or the public, or the environment.

**c) Define security.**

Security can be defined as an integrated system of activities, systems, programs, facilities, and policies for the protection of classified information and/or classified matter, unclassified controlled information, nuclear materials, nuclear weapons, nuclear weapon components, and/or the Department's and its contractors' facilities, property, and equipment.

**d) Identify the key program elements of the safeguards and security program and describe the authorities and responsibilities of each.**

*Secretary*

The Secretary

- ensures that an effective S&S program is established and executed within DOE under the authorities granted by relevant Executive orders, the U.S. Department of Energy Organization Act, and the Atomic Energy Act, and in accordance with the National Nuclear Security Administration Act;
- designates senior Department officials to direct and administer the S&S Program;
- delegates, in writing, all responsibilities and authorities as necessary to those who require them;
- approves, as the senior DOE official of the intelligence community, any Department-originated Intelligence SAPs;

- approves all other Department-originated SAPs;
- authorizes continuing operations of facilities/activities determined to be a high security risk (an authority that can only be delegated to the Deputy Secretary);
- approves and issues the DBT Policy;
- has sole jurisdiction to approve the imposition of requirements on RW programs and activities that are more stringent and/or comprehensive than those imposed by the NRC.

*Deputy Secretary*

The Deputy Secretary

- is the Chief Operating Officer of the Department, and is responsible for all Departmental policy development and operations;
- integrates corporate programs and support activities with line programs;
- reviews all staff and support office policies and guidance that affect Departmental elements.

*Under Secretary for Nuclear Security/Administrator of NNSA*

The Under Secretary for Nuclear Security/Administrator of NNSA is responsible for the management and implementation of S&S programs administered by NNSA. The Under Secretary

- authorizes continuing operations of facilities/activities determined to be a moderate security risk (an authority that can only be delegated to a head of a Departmental element).
- through the Associate Administrator for Defense Nuclear Security
  - serves as the cognizant security authority for programs, operations, and facilities under the purview of NNSA. This authority may be delegated to DOE line management and must be documented in the appropriate safeguards and security management plan.
  - authorizes NNSA federal and contractor employees to carry firearms and make arrests without warrant as provided by section 161k of the Atomic Energy Act.
  - oversees the security implementation of NNSA SAPs and provides an annual report to Congress.
  - oversees NNSA programs for technical cooperation with the International Atomic Energy Agency.
  - coordinates, as necessary, with the Office of Security and other Departmental elements, to conduct onsite S&S reviews of nuclear materials distributed abroad to the extent provided for in international, multinational, and bilateral agreements, and participates in international discussions regarding safeguards policies and procedures.
  - coordinates with Departmental elements and the Office of Security to ensure Departmental compliance with the terms of the Agreement Between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States of America and its Additional Protocol.
  - reviews and coordinates, with the Office of Security, the development of physical protection technology for the transportation of SNM, nuclear weapons, and nuclear weapons components.
  - issues direction and oversees the implementation of security conditions for operations under the cognizance of the NNSA.
  - establishes a system of control measures to assure that access to classified matter is limited to authorized persons. These control measures must be appropriate to the environment in which the access occurs and the nature of the matter. The system must include technical, physical, and personnel control measures.

- establishes procedures for reporting incidents of security concern and provides resources for conducting inquiries and damage assessments and for implementing corrective actions.
- develops and allocates the NNSA security budget, including budgets for the infrastructure that supports S&S missions.
- directs the implementation of S&S programs in accordance with the requirements of DOE O 470.4 and associated programmatic Manuals, including development of procedures and guidance.

- through the Deputy Administrator for Defense Programs
  - coordinates the required reporting of lost, potentially compromised, or unauthorized disclosure of classified information to the Joint Atomic Information Exchange Group (JAIEG).
  - requests review and approval from the JAIEG for all classified matter containing Restricted Data or Formerly Restricted Data intended for transmission to foreign entities before release.
  - ensures that security-sensitive shipments from the U.S. to other countries are coordinated with the Office of Security (i.e., shipments of SNM that are subject to DOE-administered Atomic Energy Act Mutual Defense Agreements and shipments of DOE classified matter).
  - coordinates with the Office of Intelligence on the schedule for the transportation of SNM and security-sensitive shipments.

*Under Secretary for Energy, Science, and Environment*

The Under Secretary for Energy, Science, and Environment is responsible for the management and implementation of S&S programs administered by the DOE Offices of Energy Efficiency and Renewable Energy; Environmental Management; Fossil Energy; Nuclear Energy, Science, and Technology; Civilian Radioactive Waste Management; and Science.

*Head of a Departmental Element*

The head of a Departmental element responsible for overseeing a DOE facility and the Administrator of a power marketing administration (excluding the Administrator, Bonneville Power Administration)

- develops an S&S management plan that provides a description of the organization's implementation of S&S policy and provides detailed information on the assignment of roles, responsibilities, delegations, and authorities, as well as the development of budgets and allocation of resources;
- develops S&S implementing procedures and guidance for assigned programs, implements the programs, and provides oversight and technical direction;
- develops and allocates S&S budgets for assigned programs, including budgets for the infrastructure that supports S&S missions;
- ensures that line management implement applicable S&S directives;
- notifies contracting officers of affected site/facility management contracts that must include specific S&S contractor requirements documents (CRDs);
- ensures procurement requests for new non-site-/non-facility-management contracts require inclusion of appropriate language, including the clause at 48 CFR 952.204-2, Security Requirements, and the appropriate CRDs in the resulting contracts, if necessary;

- ensures that contracting officers provide DOE F 470.1, Contract Security Classification Specification (CSCS), to the DOE cognizant security authority;
- curtails or suspends operations when continued operations would result in an unacceptable risk to national security and/or to the health and safety of DOE and contractor employees, the public, or the environment;
- integrates S&S crosscutting policies, and consistently interprets applicability of those policies to affected Departmental elements;
- ensures that the authorized security condition requirements are implemented, and remains vigilant for any local changes for affected facilities;
- ensures that S&S personnel under their cognizance are managed, trained, and equipped, and are provided the facilities and logistical support, intelligence, communications, and other support services needed to maintain protection of S&S interests;
- ensures that line management under their cognizance have implemented VA programs, and that DOE line management responsible for overseeing the program have been designated;
- ensures that implementing procedures for incidents of security concern are established and sufficient resources are provided to conduct inquiries and damage assessments and to implement corrective actions;
- designates officials responsible for conducting and completing required S&S surveys;
- ensures that contractors and their subcontractors execute applicable S&S programs and policies.

*Assistant Secretary for Environment, Safety, and Health*

The Assistant Secretary

- provides technical assistance in the development of DOE S&S policy to ensure that environmental, safety, medical, and health issues are considered;
- ensures that S&S requirements are considered in the development of policies promulgated by the Office of Environment, Safety, and Health.

*Assistant Secretary for Environmental Management*

In addition to the responsibilities under head of a Departmental element, the Assistant Secretary for Environmental Management evaluates, in coordination with the Office of Security, the adequacy of physical protection measures for irradiated reactor fuel shipments outside the U.S.

*Director, Office of Nuclear Energy, Science, and Technology*

In addition to the responsibilities under head of a Departmental element, the director authorizes the transfer of SNM to the departments of the Army, Air Force, and Navy (Navy Facilities Engineering Command only) in such quantities and at such times as necessary for new military reactor cores, existing military reactor replacement cores, and miscellaneous purposes (other than use in nuclear weapons) authorized by Congress.

*Contracting Officers*

The responsibilities of contracting officers are to

- incorporate, after notification by the DOE line management official initiating the procurement activity, appropriate CRDs into affected site/facility management contracts in accordance with law, regulation, and the DOE directives clause of the contracts;

- assist originators of procurement requests who want to incorporate the provisions of 48 CFR 952.204-2, Security Requirements, and appropriate CRDs in a new contract.

**e) Discuss the use of risk analysis as it applies to safeguards and security programs.**

Risk analysis is an analysis of safeguards and/or security system assets and vulnerabilities to establish an expected loss from certain events.

**f) Discuss the purpose of independent assessments of safeguards and security programs.**

The purpose of independent assessments of S&S programs is to

- provide assurance to the Secretary of Energy, Departmental elements, and other government agencies (OGAs) that S&S interests and activities are protected at the required levels.
- provide a basis for line management to make decisions regarding S&S program implementation activities, including allocation of resources, acceptance of risk, and mitigation of vulnerabilities. The results must provide a compliance- and performance-based documented evaluation of the S&S program.
- identify S&S program strengths and weaknesses, develop and complete a process improvement schedule, and use the results to correct and improve the overall S&S program.
- provide documentation of oversight and assessment activities.

**g) Discuss the purpose of alternative means and deviations including the following terms:**

- **Variance**
- **Waiver**
- **Exception**

There are 3 categories of deviations: variances, waivers, and exceptions. Deviations from S&S program directive requirements require approval before implementation.

Variances are approved conditions that technically vary from an Office of Security directive requirement, but afford equivalent levels of protection without compensatory measures.

Waivers are approved nonstandard conditions that deviate from a Departmental S&S program directive requirement that, if uncompensated, would create a potential or real S&S vulnerability. Waivers, therefore, require implementation of compensatory measures (e.g., additional resources to implement enhanced protection measures) for the duration of the waiver.

Exceptions are approved deviations from a Departmental S&S program directive requirement that create an S&S vulnerability. Exceptions must be approved only when correction of the condition is not feasible and compensatory measures are inadequate to preclude the acceptance of risk.

**46. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the Safeguards and Security-related aspects of DOE O 420.1A, Facility Safety.**

**a) Discuss the purpose of this Order.**

Note: DOE O 420.1A has been replaced by DOE O 420.1B, Facility Safety.

The purpose of this Order is to establish facility and programmatic safety requirements for the DOE, including the NNSA, for

- nuclear and explosives safety design criteria
- fire protection
- criticality safety
- natural phenomena hazards mitigation
- the System Engineer Program

**b) Discuss the policies and objectives of the Order.**

*Nuclear Safety Objectives*

The nuclear safety objectives of the Order are

- to ensure that new DOE hazard Category 1, 2, and 3 nuclear facilities are designed and constructed in a manner that ensures adequate protection to the public, workers, and the environment from nuclear hazards;
- to ensure that major modifications to hazard Category 1, 2, and 3 nuclear facilities comply with the design and construction requirements for new hazard Category 1, 2, and 3 nuclear facilities;
- to ensure that new DOE nuclear reactors comply with the requirements of this Order and the design requirements of DOE O 5480.30, Nuclear Reactor Safety Design Criteria.

*Explosives Safety Objectives*

The explosives safety objectives of the Order are to establish mandatory design and construction standards for safety in new DOE explosives facilities and for major modifications to such facilities. Explosives facilities include facilities and locations used for storage of, or operations with, explosives or ammunition.

**c) Given a scenario involving the design, acquisition, or maintenance of a facility, identify the safeguards and security-related sections of the general design criteria.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**d) Safeguards and security personnel should have an understanding of the safety basis documents (such as Documented Safety Analysis, Safety Analyses Reports, Hazard Analysis Reports, and Fire Hazard Analysis).**

*Document Safety Analyses (DSAs)*

Development of a DSA or preliminary documented safety analysis (PDSA) is the process whereby facility hazards are identified, controls to prevent and mitigate potential accidents

involving those hazards are proposed, and commitments are made for design, construction, operation, and disposition so as to ensure adequate safety at DOE nuclear facilities.

*Technical Safety Requirements (TSRs)*

TSRs define the performance requirements of structures, systems, and components (SSCs) and identify the safety management programs used by personnel to ensure safety. TSRs are aimed at confirming the ability of the SSCs and personnel to perform their intended safety functions under normal, abnormal, and accident conditions. These requirements are identified through hazard analysis of the activities to be performed and identification of the potential sources of safety issues. Safety analyses to identify and analyze a set of bounding accidents that take into account all potential causes of releases of radioactivity also contribute to development of TSRs.

*Hazard Analysis Report (HAR)*

A HAR documents the hazard analysis (HA) of an operation and associated activities. At a minimum, the HAR shall include the following:

- An executive summary that provides an overview of the HAR and its main conclusions
- An introduction that provides a discussion of the objectives, the scope of the analysis, the operations conducted, and the limitations and assumptions employed in the HA
- A description of the nuclear explosive and its intrinsic hazards
- A description of the nuclear explosives operations (NEOs) and the facility(ies) where the operation is to be conducted (The discussion should focus on the facility and nuclear explosive configurations and processes including equipment and tooling. The discussion should also address whether interfaces between the operation and facility have safety implications. Generic safety controls utilized during the operation should be discussed.)
- A discussion of the methodology used to conduct the HA and derive safety controls and safety requirements
- A summary of the identification of hazards and potential hazard scenarios under normal and abnormal conditions considering both internal and external environments for each step in the operations

*Fire Hazards Analysis (FHA)*

The purpose of an FHA is to comprehensively assess the risk from fire within individual fire areas in a DOE facility in relation to existing or proposed fire protection to determine if the objectives of DOE Orders are met. The FHA is developed using a graded approach, and is incorporated into the facility's safety analysis report (SAR), design-basis, and beyond-design-basis accident conditions.

A graded FHA shall contain the following elements:

- Description of construction
- Protection of essential safety class equipment
- Fire protection features
- Description of fire hazards
- Life safety considerations
- Critical process equipment
- High-value property

- Damage potential and maximum possible fire loss
- Fire department/brigade response
- Recovery potential
- Potential for a toxic, biological, and/or radiation incident due to a fire
- Emergency planning
- Security considerations related to fire protection
- Natural hazards (earthquake, flood, wind) impact on fire safety
- Exposure fire potential, including the potential for fire to spread between fire areas

**e) Safeguards and security personnel should be capable of integrating the results of the different functional area safety basis documents into safeguards and security planning documents.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**f) Safeguards and security personnel should have an understanding of the impacts of their activities on facility safety, including the use of the Unreviewed Safety Question (USQ) process whenever facility modifications are proposed as a result of deliberate act analysis or other safeguards and security requirements.**

The purpose of the USQ process is to alert DOE of events, conditions, or actions that affect the DOE-approved safety basis of the facility or operation and ensure appropriate DOE line management action. If a change is proposed or a condition is discovered that could increase the risk of operating a facility beyond that established in the current safety basis, DOE line management, including, where applicable, the NNSA, must review and determine the acceptability of that risk through the process of approving a revised safety basis that would be developed and submitted by the contractor.

**47. Safeguards and security personnel shall demonstrate a working-level knowledge of methods to maintain communication with Headquarters, field elements, regulatory agencies, the public, and other stakeholders.**

**a) Describe the Department's organization and discuss the Department's procedures for communicating between elements.**

DOE-STD-7501-99, The DOE Corporate Lessons Learned Program, states that the application of lessons learned plays a key role in maintaining Integrated Safety Management Systems (ISMSs) and in improving DOE and contractor programs, processes, and practices integral to ISMSs.

At the local level, contractor managers are expected to describe lessons learned programs as part of their Safety Management System Descriptions. These descriptions should express the local management expectations for the development, communication, and use of lessons learned. They should also describe, in whole or by reference, the infrastructure mechanisms that support development, sharing, and use of lessons learned.

The Department established Integrated Safety Management (ISM) as a Department-wide approach for managing and performing work safely. ISM defines five work-cycle functions:

(1) identifying the work, (2) analyzing the hazards, (3) defining the controls, (4) performing the work, and (5) feedback and continuous improvement. It also describes three basic levels of work within which these functions are performed: the institutional, site, and activity levels. It is expected that lessons learned will be identified, shared, and used within each function, for inter-relationships among functions, and within and among the three organizational levels of work planning and performance.

The use of lessons learned is a principal component of an organizational culture committed to continuous improvement. The methods used to instill lessons learned as part of the culture vary, as do the mechanisms for identifying, sharing, and using lessons learned.

The nature of the work and the complexity of the organization are prime determinants of cultural and infrastructure support for lessons learned. Cultural methods often include setting expectations, providing support and incentives, conducting monitoring, providing feedback, and supporting continuous improvement. Infrastructure mechanisms typically include the clear definition of resources, processes, and procedures by which personnel are supported to identify, share, and use lessons learned. The infrastructure mechanisms are often referred to as Lessons Learned Programs.

Lessons Learned Programs include two basic processes. The first is a development process that includes identification, documentation, validation, and dissemination of a lesson learned. The second is a utilization and incorporation process that includes identification of applicable lessons learned, distribution to appropriate personnel, identification of actions that will be taken as a result of the lessons learned, and follow-up to ensure that appropriate actions were taken. In addition to these elements, lessons learned programs contain processes to measure operational performance improvement and program effectiveness.

**b) Describe the Department's procedures and policy for communicating with regulatory agencies.**

The extensive and varied alliances maintenance personnel are required to cultivate require equally extensive and varied approaches. The information below provides suggested approaches, but is not all-inclusive.

DOE P 141.2, Public Participation and Community Relations, provides guidance in building alliances. This DOE policy states that public participation is open, ongoing, two-way communication, both formal and informal, between the DOE and its stakeholders concerning DOE's missions and activities. Effective public participation is at the core of good community relations, which is essential for DOE facilities to achieve their missions. Regular, interactive communication enables all parties to learn about and better understand each other's views and positions.

DOE P 141.2 also provides a mechanism for bringing a broad range of stakeholder viewpoints and community values into DOE's decision-making early in the process. This early involvement enables DOE to make more informed decisions and build mutual understanding and trust between DOE, the public it serves, and the communities that host its facilities.

Effective public participation and good community relations both rest on a foundation of positive personal relationships; DOE managers and staff are encouraged to seek to build and nurture such relationships.

The methods used to encourage public participation will vary widely in nature and scope and may include, but are not limited to, informal conversations, written and electronic communication, scheduled meetings and workshops, legally required hearings, and federal-state-local-tribal meetings. Under DOE P 141.2, DOE actively seeks, considers, and responds in a timely manner to the views of its stakeholders, thereby providing them an opportunity to influence decisions.

The goals of the DOE Public Participation and Community Relations Policy are as follows:

- DOE will actively seek to identify stakeholders, consider public input, and incorporate or otherwise respond to the views of its stakeholders in making its decisions.
- The public will be informed in a timely manner and empowered to participate at appropriate stages in DOE's decision-making processes. Such processes will be open, understandable, and consistently followed. Managers will define clear access points for public input from the earliest stages of a decision process and will provide adequate time for stakeholders to participate.
- Credible, effective public participation processes, including active community outreach, will be consistently incorporated into DOE program operations, planning activities, and decision-making processes at Headquarters and in the field. Employees within the DOE complex will share responsibility for promoting and improving public participation and community relations.
- DOE will conduct periodic reviews of its public participation and community relations efforts.

Alliances are often highly visible during emergencies. DOE G 151.1-1, volume 4-5, Emergency Facilities and Equipment, states that the ability to provide the public, media, and DOE employees with accurate and timely information is based on an effective Emergency Public Information (EPI) program. To be effective, emergency public information should be coordinated with onsite and offsite federal, state, local, and tribal emergency response organizations. The EPI program provides the means for a facility to coordinate the timely exchange of information among representatives from DOE and other organizations. This coordination is critical to prevent dissemination of confusing, conflicting, and erroneous information.

S&S interaction with Congress is often dependent on circumstances. However, DOE M 135.1-1A, Department of Energy Budget Execution Funds Distribution and Control Manual, provides some insight on congressional alliances. Congressional notifications are intended to ensure that the appropriate committees are promptly and fully informed of changes in program activities. Information may be conveyed in written correspondence or through informal discussion with the appropriate committees.

When events or conditions in the fiscal year necessitate changes to the approved budget, proposals must be communicated to the congressional committees responsible for those appropriations. Processes are in place to address changes for reprogramming, restructuring, appropriation transfer, notification, and deferral and rescission proposals.

When changes do not require formal or internal/limited reprogramming procedures, but may affect areas known to be of interest or concern to Congress, DOE will notify the appropriate committees of changes in program activities to ensure they are promptly and fully informed.

In these cases, DOE may elect to notify the appropriate committees through less formal procedures. The Office of the Chief Financial Officer's informal discussions with the appropriate committee, or a Secretarial Officer's correspondence with the appropriate committee, serves as sufficient notification of the impending actions.

**c) Demonstrate the ability to present technical ideas in general terms to the public.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**d) Define conflict and discuss the win-lose and win-win methods of conflict resolution.**

Conflict can be defined as a disagreement through which the parties involved perceive a threat to their needs, interests, or concerns.

*The Win/Win or Integrative Approach*
There are two types of negotiation process that differ fundamentally in their approach and in the relative prospects for the stability of the agreement that is reached. The first is called the integrative or win/win approach. In these negotiations, the prospects for both sides' gains are encouraging. Both sides attempt to reconcile their positions so that the end result is an agreement under which both will benefit; therefore the resultant agreement tends to be stable. Win/win negotiations are characterized by open and empathetic communications and are commonly referred to as partnership agreements.

*The Win/Lose or Distributive Approach*
The second type of negotiation process is called the distributive or win/lose approach. In these negotiations, each of the parties seeks maximum gains and therefore usually seeks to impose maximum losses on the other side. This approach often produces agreements which are inherently unstable, as represented by the triangle balance on its apex.

**e) Discuss the purpose and describe the roles and responsibilities of safeguards and security personnel for the following DOE Orders:**
- **DOE O 151.1A, Comprehensive Emergency Management System**
- **DOE O 200.1, Information Management Program**

*DOE O 151.1A, Comprehensive Emergency Management System*
Operational emergencies are defined in DOE O 151.1C, Comprehensive Emergency Management. Operational emergency occurrences are the most serious occurrences and require an increased alert status for onsite personnel and, in specified cases, for offsite authorities. The prompt notification requirements, definitions, criteria, and classifications of operational emergencies and appropriate responses are provided in DOE O 151.1C.

The following roles and responsibilities related to the management of emergency management systems apply to Departmental elements:

- Implement emergency management policy and requirements, and maintain programs and systems consistent with the policy and the requirements.
- Establish and maintain an effective, integrated emergency management program.
- Partner with the cognizant Secretarial Officers (CSOs), the Associate Deputy Secretary for Field Management, the Assistant Secretary for Environment, Safety, and Health, and the Director of Emergency Management to establish and maintain performance measures and criteria to implement this Order (DOE O 151.1A) for facilities and activities under their cognizance, and to ensure that these performance measures and criteria are incorporated in contractual arrangements.
- Approve and submit approved site emergency plans to the Director of Emergency Management and the CSO(s).
- Approve and submit approved emergency planning zones to the Assistant Secretary for Environment, Safety, and Health, the Director of Emergency Management, and the CSO(s).
- Coordinate with the CSO(s) to ensure resources are available to implement this Order for facilities and activities under their cognizance.
- Ensure the development of appropriate emergency plan implementing procedures for timely and accurate emergency classification, notification, and reporting of emergency events for facilities under their cognizance, and establish pre-authorization criteria when possible.
- Ensure emergency public information planning is integrated with the development and maintenance of emergency plans.
- Ensure effective communication systems and protocols are coordinated and maintained with the HQ emergency operations center regarding emergencies involving or affecting facilities or materials under DOE jurisdiction or requiring DOE assistance.
- Review and approve emergency readiness assurance plans (ERAP) that cover facilities under their supervision. Prepare the operations/field office annual emergency readiness assurance plan and submit it to the CSO and the Director of Emergency Management for inclusion in the annual report of the Under Secretary on the status of the emergency management system.
- Where applicable, pre-designate a DOE employee as the on-scene coordinator for federal responses under the National Contingency Plan and as the on-scene commander and/or senior energy official in accordance with the Federal Radiological Emergency Response Plan.
- Participate in the development and implementation of mutual assistance agreements with state, tribal, and local authorities.
- Ensure that hazards assessments and hazards surveys for emergency planning purposes are adequately performed and documented.
- Ensure site offices and contractors participate in a continuing emergency preparedness program of training, drills, and exercises.
- Conduct periodic assessments of facility emergency management programs and/or periodically review contractor self-assessment programs to ensure compliance with DOE directives and policy. Provide the results/conclusions to the CSO and the Director of Emergency Management, and ensure a maximum of one assessment per site per year.
- During an emergency, conduct appropriate and necessary emergency actions.
- Implement corrective actions for lessons learned from actual emergency responses and based on findings from evaluations, assessments, and appraisals.

- Establish and maintain an emergency operations center to respond to emergency events. Every DOE emergency operations center shall be equipped with compatible communication, photo/video, and automatic data processing support specified by the Director of Emergency Management.
- Ensure that emergency plans and procedures for all facilities under DOE purview are prepared, reviewed annually, and updated, as necessary, and are integrated within the overall site office emergency preparedness program.
- Assign senior representatives to the Emergency Management Advisory Committee.
- Develop, implement, maintain, and update, as necessary, an emergency management program, commensurate with the facility-specific hazards and consistent with Departmental directives and standards of performance.
- Prepare and maintain emergency plans, procedures, and technical resource capabilities that address emergency classification, notification, reporting, response actions, training and drills, exercises, emergency public information, outreach and coordination, accident investigation, applicable federal statutes, state and local laws, DOE Orders, and implementing regulations and guidance.
- Direct appropriate emergency response actions within the area under DOE control and at the scene of the emergency.
- Ensure the effectiveness of a continuing emergency preparedness program.
- Establish and maintain an internal assessment program to ensure the readiness of emergency response capabilities, including developing and conducting a self-assessment program, as well as establishing systems and measures to monitor and evaluate line performance.

*DOE O 200.1A, Information Management Program*

The objectives of this Order are to

- ensure Departmental missions and goals, information, information resources, and information technology investment decisions will be made based on programmatic need, using performance-based measures tied to the budget, using sound business practices, and complying with applicable laws and regulations;
- treat information, information resources, and information technology as corporate assets integrated with programmatic planning and budgeting;
- provide a framework for managing information, information resources, and information technology investment, which supports the operating elements of the Department in the accomplishment of its missions and functions in an efficient and effective manner and in accordance with Departmental policy.

Maintenance of records (documentation) must be in accordance with National Archives and Record Administration-approved DOE or site-specific records retention and disposition schedules per DOE O 200.1.

**f) Identify the internal and external groups with which the safeguards and security personnel interface.**

S&S personnel must interface with a variety of people including contractor personnel, fissile operating personnel, safety personnel, all levels of management, professional societies, DOE management, and the public.

**g) Describe the different types of media that may be utilized to communicate with these groups and discuss the advantages and disadvantages of each.**

These groups can be contacted through both written (e.g., letters, e-mail, white papers) and oral (e.g., by phone, face to face, via presentations) media.

**48. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of contract management and administration sufficient to appraise contractor organizations participating in the safeguards and security programs.**

**a) Discuss the key elements of the contractual relationship between the DOE and its contractors.**

DOE personnel who use the contracting process to accomplish their programs must support the contracting officer in ensuring that

- competitive sources are solicited, evaluated, and selected;
- quality standards are prescribed and met;
- performance or delivery is timely;
- prices, estimated costs, and fees are reasonable.

**b) Discuss the roles and responsibilities of safeguards and security personnel in the contract management and administration processes.**

See element "a" of this competency.

**49. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of financial management to meet commitments to quality, cost, and schedule for safeguards and security.**

**a) Define and compare the terms "cost estimate" and "budget."**

*Cost Estimate*

A cost estimate is a statement of costs estimated to be incurred in the conduct of an activity, such as a program, or in the acquisition of a project or system. The estimate can be in the form of proposals by contractors or government agencies, a response to a program opportunity notice, or a DOE estimate.

*Budget*

A budget is a statement of the financial position of an administration for a definite period of time based on estimates of expenditures during the period and proposals for financing them.

**b) Describe the process for preparing cost estimates and a budget.**

*Cost Estimates*

The techniques used for preparing cost estimates will necessarily vary with the project's phase of acquisition and degree of definition; the state-of-the-art of the project; the availability of databases, cost-estimating techniques, time, and cost estimators; and the level of detail or work breakdown structure required in the estimates. A study of the item or task,

in light of the degree of estimating difficulty, should indicate the method or combination of methods to be used in estimating the cost of that particular item or task, as follows:

- Bottom-Up Technique. Generally, a work statement and set of drawings or specifications are used to "takeoff" material quantities required to perform each discrete task performed in accomplishing a given operation or producing an equipment component. From these quantities, direct labor, equipment, and overhead costs are derived and added thereto.
- Specific Analogy Technique. Specific analogies depend upon the known cost of an item used in prior systems as the basis for the cost of a similar item in a new system. Adjustments are made to known costs to account for differences in relative complexities of performance, design, and operational characteristics.
- Parametric Technique. Parametric estimating requires historical data bases on similar systems or subsystems. Statistical analysis is performed on the data to find correlations between cost drivers and other system parameters, such as design or performance parameters. The analysis produces cost equations or cost-estimating relationships, which can be used individually or grouped into more complex models.
- Cost Review and Update Technique. An estimate is constructed by examining previous estimates of the same project for internal logic, completeness of scope, assumptions, and estimating methodology.
- Trend Analysis Technique. A contractor efficiency index is derived by comparing originally projected contract costs against actual costs on work performed to date. The index is used to adjust the cost estimate of work not yet completed.
- Expert Opinion Technique. This technique may be used when other techniques or data are not available. Several specialists can be consulted reiteratively until a consensus cost estimate is established.

Cost estimates can be developed for many purposes: comparative studies, trade-off studies, funding decisions, program changes, cost-benefit analyses, procurement support, or independent review or analysis of another estimate for a test of reasonableness. Cost estimates will include all relevant costs, depending on the purpose of the estimate (e.g., total life-cycle costs or components thereof, such as research, development, production, operating support, and decommissioning costs, as appropriate).

*Budget*

Providing adequate resources to develop, acquire, and operate a project is first a design constraint, and second a determination of the Department's planning and budgeting process. The budget decisions shall be consistent with project baseline decisions derived from requirements contained in the project management system.

Integration of decisions concerning project resource availability in the planning and budgeting process involves the following procedures:

- Field Budget Call. A field budget call shall be issued by the chief financial officer in mid-to-late January incorporating any budget planning decisions that have been made by the Secretariat. Prior to including a project in the budget, a conceptual design shall be completed. Also, any planned conceptual designs that are expected to exceed $1 million shall be completed and submitted to HQ. Project data sheets shall be developed and submitted for new project efforts and ongoing project efforts that require additional funding. This documentation and the conceptual design report shall be used to validate the project and to defend the project in the internal review budget.

- Project Validation. Shortly after the field call is issued, the Office of Program/Project Management shall issue procedures and a checklist to be used with the information received in the field budget submission to conduct project validations. In April and May, the Office of Program/Project Management, in coordination with the program offices, shall assess new projects over $5 million and ongoing projects requesting additional funding. The validation process evaluates the projects for readiness to proceed into the Department's budget process, and examines the planning, development, and baseline of a project to ensure that the funds requested are commensurate with the project's anticipated scope and schedule. Normally, the project must be validated prior to inclusion in the internal review budget.
- Internal Review, Office of Management and Budget, and Congressional Budgets. Project documentation shall be updated according to decisions made in each review. The conceptual design report, justification of mission need, and project data sheet are the mainline documents used to defend the project within the Department. Outside DOE (i.e., in OMB and Congress), only the project data sheet is used. Therefore, it is vital that the document be accurate and up to date for each review.
- Field Work Package Proposal and Authorization System. Specific DOE contractors, primarily management and operations contractors, process their budget submissions through the use of the Field Work Package Proposal and Authorization System (WPAS). The major emphasis of WPAS is to group associated research and development tasks and activities into work packages for the purpose of DOE approval and control. A work package might include several project-related efforts grouped by objectives and technical discipline. Each work package shall be measurable in terms of performance, and must include sufficient specifications of verifiable events or deliverables to mark project achievement.

**c) Describe and compare labor and non-labor costs.**

When estimating labor costs, the worker's base rate plus all payroll indirect costs (e.g., Federal Insurance Contributions Act and payroll insurance costs), are multiplied by the estimated labor hours to generate the labor cost. Typically, this sum is handled as a direct labor cost. For ease of estimating, an average crew rate can be used and rounded to the nearest even dollar hourly rate. Non-labor costs include interest, depreciation, rent, and indirect business taxes.

**d) Describe and compare direct and indirect costs.**

Direct costs are costs that can be specifically identified with a particular project or activity, including salaries, travel, equipment, and supplies directly benefiting the project or activity.

Indirect costs are costs incurred by an organization for common or joint objectives and cannot be identified with a particular project or activity. Examples are utilities, computer processing, security, and administrative expenses. Indirect costs are often referred to as overhead or burdened expenses.

**e) Discuss methods of reducing indirect costs.**

There are several ways to reduce indirect costs including the following:

- Understand the basis for allocation of cost pools.
- Question rate changes.
- Question cost changes.
- Look for inefficient/costly practices.
- Provide input to budget validations of indirect costs.
- Work with the chief financial officer for a more effective process.

**f) Discuss the types of projects and the methods for funding these projects.**

Following are different types of S&S projects:

- Operational Requirements. These include, but are not limited to, material consolidation, facility mission changes, changes in the DBT impacting site operations, PF redeployments, maintenance and testing changes, PF manning levels, procurement of technical expertise and support personnel, and additional training requirements.
- Capital Equipment. This includes, but is not limited to, alarm and assessment system components, MC&A systems, access control system components, and equipment necessary to complete the S&S mission (e.g., breaching tools, vehicles, PF armaments, additional capabilities necessary to address changes in the DBT).
- General Plant Projects (GPPs). These include, but are not limited to, alarm and assessment systems/components, MC&A systems, access control systems/components, or infrastructure improvements.
- Line Item Construction Projects. These include current and proposed projects that are not part of a GPP or capital equipment procurement, but are necessary to support S&S programs and operations.

The Resource Plan (RP) identifies S&S resources necessary to ensure protection of Department assets and identifies changes in resource requirements. The RP should contain the funding profile and the impacts if not funded for each project type listed above.

**50. Safeguards and security personnel shall demonstrate a working-level knowledge of assessment techniques (such as planning and use of observations, interviews, and document reviews) to assess facility performance, report results of assessments, and follow-up on actions taken as the result of assessments.**

**a) Describe the role of safeguards and security personnel in overseeing government-owned contractor-operated facilities.**

The role of S&S personnel is to ensure that S&S requirements necessary for a practical safeguarding of applicable DOE facilities and personnel are being adequately implemented. S&S personnel perform DOE line management oversight of their assigned facilities to ensure that

- the contractor is operating facilities safely and efficiently (i.e., within the boundaries of those controls invoked in the facility authorization basis);

- the contractor's management system is effectively controlling conduct of operations as related to nuclear safety;
- effective lines of communication between DOE and its operating contractors are maintained during periods of normal operation, and following reportable events, in accordance with DOE Orders and requirements.

**b) Describe the assessment requirements and limitations associated with safeguards and security personnel's interface with contractor employees.**

As assessment requirements and limitations associated with the interface of contractor employees vary from site to site, the local qualifying official will evaluate the completion of this competency.

**c) Conduct an interview representative of one that would be conducted during an occurrence investigation.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**d) Explain the essential elements of a performance-based assessment including investigation, fact-finding, and reporting.**

*Investigation*

It is important to begin the investigation as soon as an assessment is called for to ensure that data is not lost. The information that should be collected consists of: conditions before, during, and after operation of the facility; personnel involvement; environmental factors; and other information having relevance to the operation of the facility.

*Fact Finding*

Once all the data has been collected, the data should be verified to ensure accuracy. The basic need is to determine the direct, contributing, and root causes so that effective corrective actions can be taken that will prevent recurrence. Some areas to be considered when determining what information is needed include

- activities related to the operations of the facility
- initial or recurring problems
- hardware (equipment) or software (programmatic-type issues) associated with the facility
- recent administrative program or equipment changes
- physical environment or circumstances

Some methods of gathering information include conducting interviews and collecting statements. Interviews must be factual. Preparing questions before the interview is essential to ensure that all necessary information is obtained. Interviews should be conducted, preferably in person, with those people who are most familiar with the system. Individual statements could be obtained if time or the number of personnel involved makes interviewing impractical. Interviews can be documented using any format desired by the interviewer. Consider conducting a walk-through of the system or facility as part of the interview if time permits.

*Reporting*

Review of reports and documents helps develop the foundation for identifying weaknesses and areas that are of concern to an auditor.

Review relevant documents or portions of documents as necessary, and reference their use in support of facility operation. Record appropriate dates and times associated with the occurrence on the documents reviewed. Examples of documents include the following:

- Operating logs
- Correspondence
- Inspection/surveillance records
- Maintenance records
- Meeting minutes
- Computer process data
- Procedures and instructions
- Vendor manuals
- Drawings and specifications
- Functional retest specifications and results
- Equipment history records
- Design basis information
- Safety analysis report (SAR)/technical specifications
- Related quality control evaluation reports
- Operational safety requirements
- Safety performance measurement system/occurrence reporting and processing system (SPMS/ORPS) reports
- Radiological surveys
- Trend charts and graphs
- Facility parameter readings
- Sample analyses and results (chemistry, radiological, air, etc.)
- Work orders

**e) Describe the contents of an assessment report.**

Writing the report is documenting the result of an assessment. The purpose of a report is to provide documentation necessary to support findings and concerns identified by the assessor(s). The report should clearly state the status of reviewed areas and act as the reference for future discussions regarding corrective action plans.

Each assessment report will be unique, depending on the scope and results of the assessment. An example of a typical assessment report is shown in DOE-STD-1070-94, Guidelines for Evaluation of Nuclear Facility Training Programs, and in DOE Standard DOE-STD-3006-2000, Planning and Conduct of Operational Readiness Reviews, and includes the following sections:

- Cover page
- Summary
- Background
- Description of assessment
- Results and recommendations
- Conclusion

**f) Explain the essential elements and processes associated with the following assessment activities:**
- **Exit interviews**
- **Closure process**
- **Tracking to closure**
- **Follow-up**
- **Contractor corrective action implementation**

*Exit Interview*

Assessments can gain value from an exit interview. This interview is used primarily to present the assessment summary and provide the assessed organization an opportunity to verify the factual accuracy of assessment results. To facilitate this, assessors should be prepared to provide detailed supporting information for those results (ideally, a draft assessment report should be available at this time). This interview also offers an opportunity for the assessed organization to present its management position and any plans for addressing the results. Reasonable time should be allowed to discuss any concerns, but this interview should not be used to argue the assessment agenda or methodology.

*Closure Process*

In the closure process, contractors send a letter to the directives management group (DMG) requesting closure and stating that the corrective actions in the implementation plan have been completed. The DMG coordinates approval of the closure with the appropriate division of primary interest and the contracting officer's representative.

*Tracking to Closure*

After a reasonable period of time has elapsed, follow-up activities should be performed to verify the effectiveness of the corrective action and how it was implemented. This is referred to as tracking to closure. There are several ways to verify the implementation of corrective action, including
- a reassessment of the deficient areas;
- review of new or revised quality-affecting documents such as manuals, procedures, and training records;
- verification during the next scheduled assessment;
- verification by conducting a surveillance covering the areas of concern.

The key point to remember when verifying corrective action implementation is that verification is necessary. A solution to a problem may look good on paper but may not be easily implemented. The failure to adequately identify all root causes will most likely result in a recurrence of the deficiency. Therefore, an appropriate amount of follow-up is necessary to assure the effectiveness of the corrective action process and to reestablish confidence in the item/service assessed.

*Follow-Up*

After a reasonable period of time has elapsed, follow-up activities should be performed to verify the effectiveness of the corrective actions and how they were implemented. The verification should, at a minimum, sample the corrective actions to determine whether the problem/issue to be addressed has been resolved. The organization's reporting systems (e.g., noncompliance tracking system, occurrence reporting and processing system, external

oversight reports and regulatory violations, performance indicators) should be reviewed for evidence of the problem (or a similar problem) recurring. The same techniques used to conduct assessments may be used for verifying corrective actions; however, there are several common ways to verify the implementation of corrective actions, including the following:

- Reassessment of the deficient areas
- Review of new or revised quality-affecting documents such as manuals, procedures, and training records
- Verification during the next scheduled assessment
- Verification by conducting a surveillance covering the areas of concern

*Contractor Corrective Action Implementation*

Management responsible for the activities assessed is also responsible for the development of effective corrective action of the problem areas or deficiencies discovered during the assessment. At a minimum, the corrective action should address

- measures to correct each deficiency
- identification of all root causes for significant deficiencies
- determination of the existence of similar deficiencies
- corrective actions to preclude recurrence of like or similar deficiencies
- assignment of corrective action responsibility
- completion dates for each corrective action

For independent assessments, the proposed corrective action should be reviewed for concurrence by the assessment team leader. This will help ensure that the planned actions will be effective in resolving the problem areas and deficiencies reported by the assessment team.

**g) Describe the actions to be taken if the contractor challenges the assessment findings and explain how such challenges can be avoided.**

Disputes over the assessment findings, the corrective action plan, or its implementation (such as timeliness or adequacy) must be resolved at the lowest possible organizational level. The organization that disagrees with the disposition of a given issue may elevate the dispute for timely resolution. The organization that disagrees with the disposition of a given issue must elevate the dispute in a step-wise manner through the management hierarchy. The dispute must be raised via a deliberate and timely dispute resolution process that provides each party with equal opportunity for input and a subsequent opportunity to appeal decisions up to the Secretary of Energy, if necessary.

**h) Participate in formal meetings between DOE management and senior contractor management to discuss results of safeguards and security assessments.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**51. Safeguards and security personnel shall demonstrate a working knowledge of problem analysis and techniques necessary to identify problems, determine potential causes of problems, and identify corrective action.**

**a) Describe and explain the application of problem analysis techniques including the following:**

- **Root cause analysis**
- **Causal factor analysis**
- **Change analysis**
- **Barrier analysis**
- **Management oversight risk tree analysis**

*Root Cause Analysis*

Any root cause analysis method that includes the following basic steps may be used for problem analysis:

- Identify the problem. Remember that actuation of a protective system constitutes the occurrence but is not the real problem; the unwanted, unplanned condition or action that resulted in actuation is the problem to be solved. For example, dust in the air actuates a false fire alarm. In this case, the occurrence is the actuation of an engineered safety feature. The smoke detector and alarm functioned as intended; the problem to be solved is the dust in the air, and not the false fire alarm. Another example is when an operator follows a defective procedure and causes an occurrence. The real problem is the defective procedure; the operator has not committed an error. However, if the operator had been correctly trained to perform the task and, therefore, could reasonably have been expected to detect the defect in the procedure, then a personnel problem may also exist.
- Determine the significance of the problem. Were the consequences severe? Could they be next time? How likely is recurrence? Is the occurrence symptomatic of poor attitude, a safety culture problem, or some other widespread program deficiency? Base the level of effort of subsequent steps of your assessment upon the estimation of the level of significance.
- Identify the causes immediately preceding and surrounding the problem.
- Identify the reasons why the causes in the preceding identification step existed, working your way back to the root cause (the fundamental reason that, if corrected, will prevent recurrence of this and similar occurrences throughout the facility and other facilities under your control). This root cause is the stopping point in the assessment of causal factors. It is the place where, with appropriate corrective action, the problem will be eliminated and will not recur.

*Causal Factor Analysis*

Causal factor analysis is used for multi-faceted problems or long, complex causal factor chains. Cause and effects diagrams describe the time sequence of a series of tasks and/or actions and the surrounding conditions leading to an event. The event line is a time sequence of actions or happenings, while the conditions are anything that shapes the outcome ranging from physical conditions (such as an open valve or noise) to attitude or safety culture. The events and conditions as given on a chart describe a causal factor chain.

*Change Analysis*

Change analysis looks at a problem by analyzing the deviation between what is expected and what actually happened. The evaluator essentially asks what differences occurred to make the outcome of this task or activity different from all the other times this task or activity was successfully completed. This technique consists of asking the questions: What? When?

Where? Who? How? Answering these questions should provide direction toward answering the root cause determination question: Why? Primary and secondary questions included within each category will provide the prompting necessary to thoroughly answer the overall question. Some of the questions will not be applicable to any given condition. Some amount of redundancy exists in the questions to ensure that all items are addressed. Key elements to address include the following:

- Consider the event containing the undesirable consequences.
- Consider a comparable activity that did not have the undesirable consequences.
- Compare the condition containing the undesirable consequences with the reference activity.
- Set down all known differences whether they appear to be relevant or not.
- Analyze the differences for their effects in producing the undesirable consequences. This must be done with careful attention to detail, ensuring that obscure and indirect relationships are identified (e.g., a change in color or finish may change the heat transfer parameters and consequently affect system temperature).
- Integrate information into the investigative process relevant to the causes of, or the contributors to, the undesirable consequences.

Change analysis is a good technique to use whenever the causes of the condition are obscure, you do not know where to start, or you suspect a change may have contributed to the condition. Not recognizing the compounding of change (e.g., a change made five years previously combined with a change made recently) is a potential shortcoming of change analysis. Not recognizing the introduction of gradual change as compared with immediate change also is possible. This technique may be adequate to determine the root cause of a relatively simple condition. In general, though, it is not thorough enough to determine all the causes of more complex conditions.

*Barrier Analysis*

There are many things that should be addressed during the performance of a barrier analysis. The questions listed below are designed to aid in determining what barrier failed, thus resulting in the occurrence.

- What barriers existed between the second, third, etc., condition/situation and the second, third, etc., problems?
- If there were barriers, did they perform their functions? How?
- Did the presence of any barriers mitigate or increase the occurrence severity? Why?
- Were any barriers not functioning as designed? Why?
- Was the barrier design adequate? How?
- Were there any barriers in the condition/situation source(s)? Did they fail? Why?
- Were there any barriers on the affected component(s)? Did they fail? Why?
- Were the barriers adequately maintained?
- Were the barriers inspected prior to expected use?
- Why were any unwanted energies present?
- Is the affected system/component designed to withstand the condition/situation without the barriers? Why?
- What design changes could have prevented the unwanted flow of energy? Why?
- What operating changes could have prevented the unwanted flow of energy? Why?

- What maintenance changes could have prevented the unwanted flow of energy? Why?
- Could the unwanted energy have been deflected or evaded? How?
- What other controls are the barriers subject to? Why?
- Was this event foreseen by the designers, operators, maintainers, anyone?
- Is it possible to have foreseen the occurrence? Why?
- Is it practical to have taken further steps to have reduced the risk of the occurrence?
- Can this reasoning be extended to other similar systems/components?
- Were adequate human factors considered in the design of the equipment?
- What additional human factors could be added? Should be added?
- Is the system/component user friendly?
- Is the system/component adequately labeled for ease of operation?
- Is there sufficient technical information for operating the component properly? How do you know?
- Is there sufficient technical information for maintaining the component properly? How do you know?
- Did the environment mitigate or increase the severity of the occurrence? How?
- What changes were made to the system/component immediately after the occurrence?
- What changes are planned to be made? What changes might be made?
- Have these changes been properly, adequately analyzed for effect?
- What related changes to operations and maintenance have to be made now?
- Are expected changes cost effective? Why? How do you know?
- What would you have done differently to have prevented the occurrence, disregarding all economic considerations (as regards operation, maintenance, and design)?
- What would you have done differently to have prevented the occurrence, considering all economic concerns (as regards operation, maintenance, and design)?

Barrier analysis is a systematic process that can be used to identify physical, administrative, and procedural barriers or controls that should have prevented the occurrence. This technique should be used to determine why these barriers or controls failed and what is needed to prevent recurrence.

*Management Oversight Risk Tree Analysis*

Management oversight risk tree (MORT) analysis is used to prevent oversight in the identification of causal factors. It lists on the left side of the tree specific factors relating to the occurrence, and on the right side of the tree, it lists the management deficiencies that permit specific factors to exist. The management factors all support each of the specific barrier/control factors. Included is a set of questions to be asked for each of the factors on the tree. As such, it is useful in preventing oversight and ensuring that all potential causal factors are considered. It is especially useful when there is a shortage of experts to ask the right questions. However, because each of the management factors may apply to the specific barrier/control factors, the direct linkage or relationship is not shown but is left up to the analyst. For this reason, causal factor analysis and MORT should be used together for serious occurrences: one to show the relationship, the other to prevent oversight.

**b) Describe and explain the application of the following root cause analysis processes in the performance of occurrence investigations:**

- **Events and causal factor charting**
- **Root cause coding**
- **Recommendation generation**

*Events and Causal Factors Charting*

Events and causal factor analysis is used for multi-faceted problems or long, complex causal factor chains. The resulting chart is a cause and effects diagram that describes the time sequence of a series of tasks and/or actions and the surrounding conditions leading to an event. The event line is a time sequence of actions or happenings while the conditions are anything that shapes the outcome ranging from physical conditions (such as an open valve or noise) to attitude or safety culture. The events and conditions as given on the chart describe a causal factor chain. The direct, root, and contributing cause relationships in the causal factor chain are shown in figure 1.

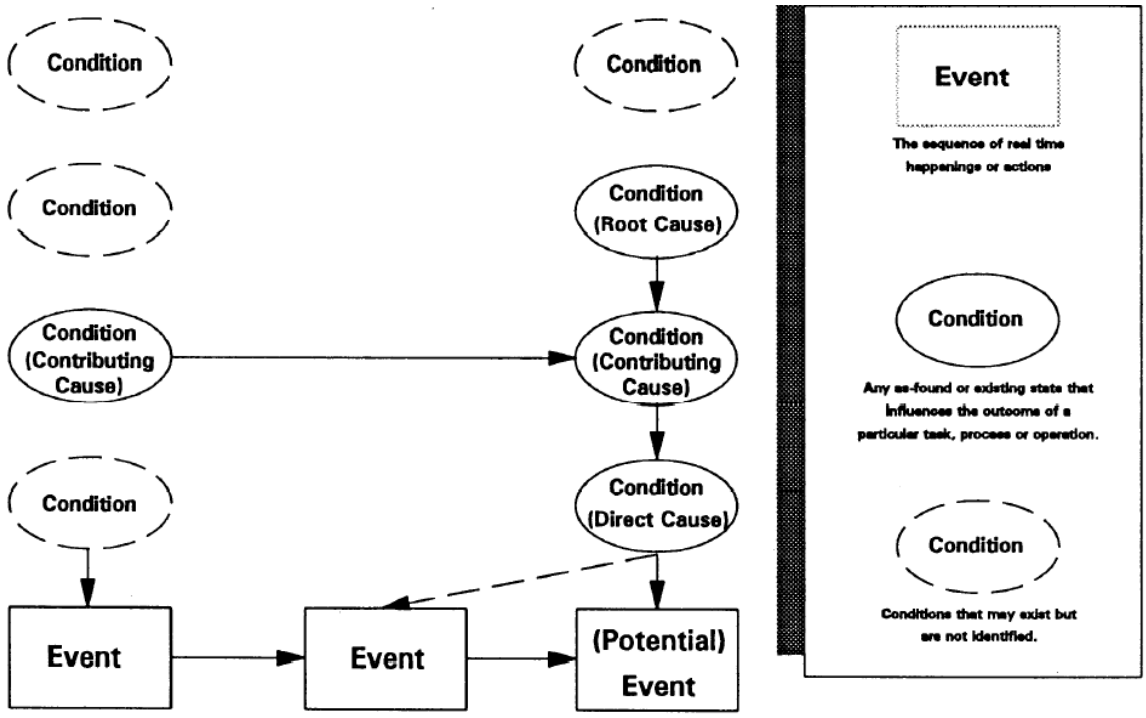


**Figure 1. Causal factor relationships**

*Root Cause Coding*

All causes must be identified as required in DOE M 231.1-2, Occurrence Reporting and Processing of Operations Information, section 11, Occurrence Reporting Model, and included in the occurrence report. The cause codes to be used for reporting are provided in the causal analysis tree, which is also in section 11 of DOE M 231.1-2. Guidance on selecting the appropriate cause code is provided in DOE G 231.1-2, Occurrence Reporting Causal Analysis Guide. The cause description field should include a brief discussion to clearly link the event to the cause code(s).

For those occurrences that require a formal root cause analysis, any of the site approved root cause analysis methodologies are permitted. The methodology used must be included in the cause description field of the occurrence report.

*Recommendation Generation*

Following identification of the root causes for a particular causal factor, achievable recommendations for preventing its recurrence are then generated. The root cause analyst is often not responsible for the implementation of recommendations generated by the analysis. However, if the recommendations are not implemented, the effort expended in performing the analysis is wasted. In addition, the events that triggered the analysis should be expected to recur. Organizations need to ensure that recommendations are tracked to completion.

**c) Describe the following types of investigations and discuss an example of the application of each:**
- **Type A**
- **Type B**
- **Type C**

A Type A investigation is conducted for the more serious accidents and is appointed and managed by the Office of the Assistant Secretary for Environment, Safety, and Health. A Type B investigation is appointed and managed at the field level. However, the elements of the investigation and the report format are the same.

Type A investigations include the following:
- A fatality
- Three serious injuries
- An exposure of roughly five times the dose guidelines
- A hazardous materials release of five times the reportable quantity
- $2.5 million in property damage
- An accidental criticality
- Loss or theft that constitutes a hazard
- Any accident or series of accidents for which a Type A investigation is deemed appropriate by the Secretary or the Assistant Secretary for Environment, Safety, and Health

Type B investigations include the following:
- One five-day hospitalization
- A series causing five lost workday cases in a year
- Exposure of roughly two times the dose guidelines
- A hazardous materials release of two times the reportable quantity
- $1 million in property damage
- Any accident or series of accidents for which a Type B investigation is deemed appropriate by the Secretary, the Assistant Secretary for Environment, Safety, and Health, the Associate Deputy Secretary for field management, the cognizant Secretarial Officer, or the head of the field element

Type C investigations are no longer in use.

**d) Compare and contrast immediate, short-term, and long-term actions taken as the result of problem identification or an occurrence.**

Immediate actions are to put the system or process into a safe and stable condition. Short-term actions are generally recovery actions to allow other nearby processes or systems to return to operation, or to return unaffected portions of the same process to operation. Short-term actions may also be appropriate if only a few items are involved in the occurrence, and the correction path can be readily determined. They are likely to involve things such as shift orders, standing orders, and temporary modifications. Short-term actions usually do not deal with recurrence control, or may have expensive compensatory actions for recurrence control. Long-term actions may involve engineered solutions and more deliberately revised procedures and training, and usually are undertaken to ensure recurrence control.

**e) Describe various data gathering techniques and the use of trending/history when analyzing problems.**

Typical data gathering techniques for the typical problems discovered in oversight or from contractor incidents include the following:

- A review of similar problems, the lessons learned database, and the operating experience weekly summaries can lead to workable ways of solving an issue.
- Document searches and reviews can provide useful information. The type of problem being investigated may be evident from site or nationwide documentation. Previous solutions and their utility may be identified. Document reviews may have trails to root or contributing causes.
- Interviews can provide insight into staff morale, general safety attitudes, and sight culture that may have led to problems, may be precursor conditions, or that can identify areas that need watching.
- Numerical, electronic, and database record reviews are helpful if looking for trends.
- Statistical screening techniques, rank correlations, control charts, and other statistical techniques can be useful in detecting trends and determining if a trend actually exists.
- Other safety analysis techniques such as event trees, fault trees, timelines, and what if techniques can be applied in retrospect to look for causes and contributing factors.

**52. Safeguards and security personnel shall demonstrate the ability to apply problem analysis techniques necessary to identify problems, determine potential causes of problems, and identify corrective action.**

**a) Given event and occurrence data, apply problem analysis techniques and identify the problems and how they might have been avoided.**

**b) Participate in a Type A, B, or C investigation.**

**c) Participate in a contractor or DOE problem analysis and critique the findings and results.**

**d) Using data, interpret two fault tree analyses.**

Elements “a” through “d” are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**53. Safeguards and security personnel shall demonstrate the ability to trend contractor performance related to safeguards and security in accordance with the following Department of Energy directives:**

- **DOE O 210.1, Performance Indicator and Analysis of Operations Information**
- **DOE O 231.1, Environmental, Safety, and Health Reporting**
- **DOE M 231.1-1 (231.1-2), Environmental, Safety, and Health Reporting Manual**

**a) Discuss the key processes used in trending and analysis of safeguards and security information.**

Systematic analysis should be used to determine and correct the root causes of unplanned occurrences related to S&S. S&S provides guidance for collecting and trending maintenance history for recurring or persistent problems that should be reviewed by the analysis program. An analysis program may be used effectively to reduce recurring S&S problems by identifying and resolving root causes of the problem.

**b) Using an actual list of performance indicators, e.g., security infractions/violations, property loss, or inventory deficiencies, determine what type of assessments should be performed and in what areas.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**c) Given a set of incident/occurrence report data for a specified period, analyze the information for safeguards and security performance, trends, or compliance problems.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

**54. Safeguards and security personnel shall demonstrate the ability to assess the contractor's ability to develop program plans in accordance with DOE O 470.1, Safeguards and Security Program.**

**a) Assess the contractor's Site Safeguards and Security Plan for inclusion of sitewide Master Safeguards and Security Agreements, Facility Descriptions and Operational Plans, and Resource Plans.**

**b) Assess the contractor's facility descriptions and operational plans to ensure that the plans describe the site protection strategies, facility protection systems, and programs currently in place.**

**c) Assess the contractor's ability to ensure that it presents a five-year projection of the upgrades and their associated costs in addressing the vulnerabilities and risks.**

**d) Assess the contractor's ability to ensure that performance levels are based on performance indicators such as vulnerability assessments, system performance tests, surveys, inspections, evaluations, and training levels.**

**e) Assess supporting documentation (vulnerability assessments, cost/benefit analyses, implementation procedures, guidelines, performance exercises, etc.).**

Elements "a" through "e" are performance-based competencies. The qualifying official will evaluate the completion of these competencies.

**55. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of approvals and surveys in accordance with DOE O 470.1, Chapter IX, Survey Program.**

Note: DOE O 470.1, Chapter IX, Survey Program, has been cancelled. The information provided in this competency statement was taken from DOE M 470.4-1, Safeguards and Security Program Planning and Management.

**a) Describe the approval process of a new facility or interest at a Department facility.**

Initial surveys must be conducted at facilities where there will be a facility clearance established for a facility with an importance rating of A, B, C, or PP. Survey activities must be comprehensive and result in a satisfactory composite rating prior to a facility clearance (FCL) being granted.

**b) Discuss the safeguards and security survey process.**

Surveys and self-assessments must provide an integrated evaluation of all topical and subtopical areas to determine the overall status of the S&S program and to ensure the objectives of this section are met. The integrated evaluation is a comprehensive, synergistic approach using multiple S&S program elements that ensures total system effectiveness and, if properly implemented, will meet the required objectives. The scope of these activities and the methods used must include those listed below:

- Compliance. Compliance reflects the status of the S&S program as measured against implementation of applicable federal statutes, regulations, policies, approved SSSPs/SSPs, and other approved security plans.
- Performance. Performance indicates the degree to which the elements of the S&S program meet protection objectives based on the operational testing of program elements.
- Comprehensiveness. Comprehensiveness identifies the breadth of protection afforded all activities and interests within a facility. This is accomplished by an evaluation of the adequacy and effectiveness of programs and a thorough examination of the implementation of policies, practices, and procedures to ensure compliance and performance. All applicable topical areas identified on DOE F 470.8, Survey/Inspection Report, must be evaluated.
- Other. The scope of special and termination surveys is determined by the DOE cognizant security authority in coordination with the surveying office. Determinations of survey scope are predicated on the nature or status of operations at the facility, activity, or element being surveyed. These surveys may not cover all topical areas identified on DOE F 470.8.

**c) Discuss the ratings given during a safeguards and security survey.**

Ratings must be based on the effectiveness and adequacy of the program at a facility, and must reflect a balance of performance and compliance results, as well as the impact of the deficiency(ies) (e.g., findings, IG recommendations) and mitigating factors. The ratings listed below must be used for all surveys (except termination), reviews, and self-assessments. Does Not Apply (DNA) and Not Rated (NR) may also be used in applicable situations.

*Types of Ratings*

- Satisfactory. The element being evaluated meets protection objectives or provides reasonable assurance that protection objectives are being met.
- Marginal. The element being evaluated partially meets protection objectives or provides questionable assurance that protection objectives are being met.
- Unsatisfactory. The element being evaluated does not meet protection objectives or does not provide adequate assurance that protection objectives are being met.
- Inspection Ratings. "Effective Performance," "Needs Improvement," and "Significant Weaknesses" are indicators of a management system performance level as outlined in DOE O 470.2B, Independent Oversight and Assurance Program, dated October 31, 2002.

*Rating Determinations*

- Existing Conditions. Ratings must be based on existing conditions at the end of the survey and not on future or planned corrective actions or conditions.
- Impact. Ratings must be based on the impact of all open deficiencies, regardless of the source.
- Marginal or Unsatisfactory Ratings. Less than satisfactory ratings in any topical area must be based on validated weaknesses in the S&S system or deficiencies in performance.
- Topical Area Ratings. A topical area rating must not be marginal for consecutive survey periods and will be assigned an unsatisfactory rating unless one of the following conditions applies:
  - The current survey of the topical area results in a satisfactory rating.
  - The previous survey that resulted in a marginal rating identified different deficiencies and reasons for the rating.
  - The deficiencies and reasons that were the basis for the previous marginal rating were related to the completion of a line item construction project or upgrade program. (In this case, acceptable interim measures must have been implemented, physically validated pending completion of the project, and documented in the survey report.)

*Subtopical Ratings*

The decision whether or not to use all subtopical ratings must be documented in local procedures. Regardless of the rating method used, the report must include the evaluation of all required subtopical areas which must be used as part of the appropriate topical area rating justification and rationale.

*Justification and Rationale*

All ratings must be supported and documented to include the rating justification and rationale.

**d) Discuss the appropriate follow-up actions necessary for each type of survey rating.**

*Notifications and Actions for Less Than Satisfactory Survey Composite Ratings*

When the survey composite ratings are less than satisfactory, the following notifications and actions must occur:

- Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, the DOE cognizant security authority must ensure SSIMS is updated and must provide the applicable Departmental elements and OGAs with the following:
  - A statement identifying the vulnerabilities and the rationale for the rating
  - Description of the corrective action/compensatory measures taken to date
  - A statement acknowledging physical validation of the adequacy of items

If the surveying office is not the same as the DOE cognizant security authority, the surveying office must notify the DOE cognizant security authority of results prior to departure from the site.

- Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of Unsatisfactory, the DOE cognizant security authority must coordinate with the Departmental element to take one of the following actions:
  - Suspend the activity and/or the FCL pending remedial action.
  - Provide the justification for continuing this critical operation to the Office of Security, the Departmental element, and as directed, other applicable Departmental elements, and identify and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.

*Notifications and Actions for Less Than Satisfactory Self-Assessment Composite Ratings*

Actions required in response to less than satisfactory self-assessment composite ratings are listed below:

- Marginal Ratings. Within 15 working days of the determination of a marginal composite rating, notification must be made to line management that includes the following:
  - A statement identifying the vulnerability and rationale for the rating
  - A description of the corrective action/compensatory measures taken to date
  - A statement acknowledging physical validation of the adequacy of items
- Unsatisfactory Ratings. Within 24 hours of determination of an overall composite rating of unsatisfactory, the cognizant security authority must coordinate with the DOE cognizant security authority, which in turn must coordinate with the Departmental element to take the following actions:
  - Suspend the activity and/or recommend suspension of the FCL pending remedial action.
  - Provide justification for continuing operations to the DOE cognizant security authority, and evaluate those immediate interim corrective actions being undertaken to mitigate identified risks or vulnerabilities.
  - If the results of a self-assessment identify an incident of security concern, it must be reported in accordance with appropriate procedures.

**56. Safeguards and security personnel shall demonstrate a familiarity-level knowledge of the general principles of project management as described in DOE Order 4700.1, Project Management System.**

**a) Discuss the purpose and requirements of the order.**

DOE Order 4700.1 has been cancelled.

**b) Discuss the responsibilities of safeguards and security personnel participating in the DOE project management system in terms of the administration and coordination of the safeguards and security programs.**

The purpose of program administration is to establish and maintain effective organizational management and control of the S&S program. For effective program management, administrators are given authority and resources commensurate with the responsibility to develop, implement, and maintain an integrated and comprehensive S&S program.

S&S program administrators should use DOE G 151.1-1, volume 5-1, Program Administration, and other guides to define their responsibilities and identify the various activities they are responsible for implementing.

**57. Safeguards and security personnel shall demonstrate a working-level knowledge of effective negotiation skills.**

**a) Discuss the essential elements of effective negotiation.**

Negotiation is a peaceable procedure for reconciling and/or compromising known differences. It is the antithesis of force and violence. A negotiation can be fruitful or completely meaningless, depending upon the existence of two essential elements. There are other less important elements, but two are absolutely essential.

These two elements are good faith and flexibility. Both must be present on both sides of the table — one without the other on either side is a fatal defect. Obviously, differences of opinion or disagreement must exist or there would be no need for a negotiation in the first place. In this situation, the parties have concluded that they should try and act as grown and mature individuals and attempt to settle their differences amicably through negotiation. Good faith and flexibility cover many facets. Good faith is meant to convey an honest desire to reach agreement on the differences that exist through compromise and a realization that the agreement thus reached should be fair and reasonable for both sides if the agreement is to endure.

A negotiation must not be viewed as an adversary proceeding, such as a case in court, where one party wins and the other loses. If one party at the table is trying to take an unfair advantage of the other party, the element of good faith is not present; hence you have no real negotiation.

The second essential element of flexibility is the heart of a negotiation. In every negotiation it must be assumed — unless you are dealing with juveniles — that your opposite numbers will always table maximum positions first. Equally important, it must be assumed — unless

you are dealing with fools — that your opposite numbers have not disclosed their minimum positions in any manner. The challenge to the able negotiator, therefore, is to start with the tabled maximum positions, and by skillfully using all of the tools in his/her kit, reach the essence or basic minimum positions upon which an agreement can and should be concluded.

If a negotiator is unable to obtain any concessions whatsoever from the tabled positions, then either the element of flexibility is missing or the negotiator is inept, in which event you find yourself with no negotiation at all. As in the case of good faith, it may be difficult and time consuming to convince yourself that what you are facing is a set of non-negotiable demands, but here again a good negotiator will see the handwriting on the wall and eventually realize just the situation he/she is in. The crucial and delicate question to be considered by the negotiator is: Are the opponents still negotiating for advantage or are their positions truly flexible, as they appear to be?

The proof of good faith and flexibility is established at the negotiating table, but not by self-serving statements or protestations either before or during the negotiations. A good negotiator knows that only by tangible manifestations can these elements be shown to exist.

**b) Describe how to develop and use strategies of negotiation.**

A good negotiator will make a list of all points to be negotiated. This is a helpful precaution that can later be used as a checklist to ensure that nothing has been overlooked or forgotten. The negotiator should determine and clearly categorize which of the points to be negotiated are "must" points and which are "give" points.

In any genuine negotiation where flexibility exists, there will always be — on both sides of the table — certain points or objectives without which the contract or agreement cannot be signed. These are referred to as "must" positions. Additionally, there will always be — on both sides of the table — other positions which are sought but which will not be insisted upon in toto, in order to reach the overall final agreement. These are referred to as "give" points. The negotiator should determine the maximum and minimum positions with respect to each point to be negotiated for both "must" and "give" points.

There are two distinct types of negotiations. First, there is the type whereby one or both sides know exactly what the other side wants before going to the negotiating table, and second, there is the type whereby both sides have agreed on a general objective, but the actual positions of each side are not known until the parties reach the table. Put yourself through a "devil's advocate" exercise whereby you test your points and positions to see if they are fair and reasonable to both sides.

**c) Describe how the following pre-negotiation elements are accomplished and developed:**

- **Objectives/desired outcomes**
- **Information gathering**
- **Analysis of the other party's objectives**
- **Identify the needs of both parties**

*Objectives/Desired Outcomes*

Determine and reduce to writing your maximum and minimum positions with respect to each point to be negotiated for both "must" and "give" points.

*Information Gathering*

There is no substitute for hard and thorough home work in preparation for a negotiation. Negotiations, like anything else, require many hours of time and preparation to back up one hour of actual time at the table.

*Analysis of the Other Party's Objectives*

Thoroughly research your opposition's background, reputation, history, performance record on previous agreements or contracts, etc. The information thus developed should be filed away for use at the table, and a good negotiator will never go to the table without it. This background information can be used during the negotiations to secure and maintain the psychological advantage necessary from time to time. Remember also that the other side will know chapter and verse concerning your own history, background, performance, etc., and will use this knowledge against you at the table.

*Identify the Needs of Both Parties*

Inherent in this exercise is respect for your opponent's positions. The existence of "good faith" on both sides, without which the negotiation is futile, assumes respect, albeit not concurrence, for the positions of both sides. The best way to test your points and positions is to put yourself in the other's position and ask yourself what you would do. Would you agree, could you agree, etc., to what you are proposing?

**d) Participate in negotiation activities with peers, DOE management, and contractor personnel.**

This is a performance-based competency. The qualifying official will evaluate the completion of this competency.

# Acronyms

| | |
|---|---|
| AIS | automated information system |
| ANACI | Access National Agency Check and Inquiries |
| ACL | adversary capabilities list |
| ACREM | accountable classified removable electronic media |
| ASTM | American Society for Testing and Materials |
| C | confidential |
| C/NSI | confidential/national security information |
| CAS | central alarm stations |
| CFR | Code of Federal Regulations |
| CI | counterintelligence |
| CM | configuration management |
| CPCI | central personal clearance index |
| CPI | critical program information |
| CRD | contractor requirements document |
| CSCS | contract security classification specification |
| CSO | cognizant secretarial officer |
| DAA | Designated Approving Authority |
| DBT | design basis threat |
| DCID | Director of Central Intelligence Directive |
| DEAR | Department of Energy Acquisition Regulation |
| DMG | Directives Management Group |
| DNA | does not apply |
| DOD | Department of Defense |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DSA | documented safety analysis |
| DSS | defense security service |
| EA | exclusion area |
| ECI | export controlled information |
| EPI | emergency public information |
| ERAP | emergency readiness assurance plan |
| F | form |
| FA | federal agent |
| FBI | Federal Bureau of Investigation |
| FCL | facility clearance |
| FGI | foreign government information |
| FHA | fire hazards analysis |
| FII | foreign intelligence information |
| FOCI | foreign ownership, control, or influence |
| FOIA | Freedom of Information Act |
| FO | federal officer |
| FRD | formerly restricted data |
| GPP | general plant project |
| GSA | General Services Administration |

| | |
|---|---|
| HA | hazard analysis |
| HAR | hazard analysis report |
| HQ | headquarters |
| IAA | Interim Access Authorization |
| IAEA | International Atomic Energy Agency |
| ID | identification |
| IDS | intrusion detection system |
| IMI | impact measurement index |
| ISCR | information systems certification report |
| ISM | integrated safety management |
| ISMS | integrated safety management system |
| ISOM | information systems security operations manager |
| ISPM | information systems security program manager |
| ISSM | information systems security site manager |
| ISSO | information systems security officer |
| ISSP | information systems security plan |
| IV&V | independent validation and verification |
| JA | job analysis |
| JAIEG | Joint Atomic Information Exchange Group |
| LA | limited area |
| MAA | material access area |
| MBA | material balance area |
| MBR | material balance report |
| MC&A | material control and accountability |
| MORT | management oversight risk tree |
| NACC | national agency check with credit |
| NACLC | national agency check with law and credit |
| NATO | North Atlantic Treaty Organization |
| NEO | nuclear explosives operation |
| NFPA | National Fire Protection Association |
| NMMSS | Nuclear Materials Management and Safeguards System |
| NMR | nuclear materials representative |
| NNPI | naval nuclear propulsion information |
| NNSA | National Nuclear Security Administration |
| NOCONTRACT | no dissemination to contractors |
| NOFORN | no foreign dissemination |
| NP | non-possessing |
| NR | not rated |
| NRC | Nuclear Regulatory Commission |
| NSI | national security information |
| NSTISSD | National Security Telecommunications and Information Systems Security Directive |
| OC | operations center |
| OCI | office of counterintelligence |
| ODNCI | office of defense nuclear counterintelligence |
| OGA | other government agency |
| OMB | office of management and budget |

| | |
|---|---|
| OPSEC | operations security |
| ORCON | originator controlled |
| ORPS | occurrence reporting and processing system |
| OST | office of secure transportation |
| OUO | official use only |
| PA | protected area |
| PDSA | preliminary documented safety analysis |
| PF | protective force |
| PIDAS | perimeter intrusion detection assessment system |
| PIN | personal identification number |
| PIR | passive infrared |
| POC | point of contact |
| PP | property protection |
| PPA | property protection area |
| PROPIN | proprietary information |
| PSAP | personnel security assurance program |
| PSI | personnel security interview |
| RD | restricted data |
| REL TO | release to country |
| RIS | reporting identification symbol |
| RP | resource plan |
| S | secret |
| S&S | safeguards and security |
| SA | special agent |
| SAP | special access program |
| SAPF | special access program facility |
| SAR | safety analysis report |
| SAS | secondary alarm station |
| SC | office of science |
| SCI | sensitive compartmented information |
| SCIF | sensitive compartmented information facility |
| SECON | security condition |
| SNM | special nuclear material |
| SO | security officer |
| SPMS | safety performance measurement system |
| SPO | security police officer |
| SPR | Strategic Petroleum Reserve |
| SRT | special response team |
| SSBI | single-scope background investigation |
| SSCs | structures, systems, and components |
| SSIMS | Safeguards and Security Information Management System |
| SSP | site security plan |
| SSSP | site safeguards and security plan |
| TID | tamper indicating device |
| TRF | Tactical Response Force |
| TSCM | technical surveillance countermeasure |

| | |
|---|---|
| TSFRD | top secret formerly restricted data |
| TSR | top secret restricted |
| TSRD | top secret restricted data |
| U | unclassified |
| U.K.-C | United Kingdom, Classified |
| UCI | unclassified controlled information |
| UCNI | unclassified controlled nuclear information |
| VA | vulnerability assessment |
| VTR | vault-type room |
| WNINTEL | warning notice intelligence sources and methods |
| WPAS | work package proposal and authorization system |

# Selected Bibliography and Suggested Reading

10 CFR 710, "Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material." January 1, 2006.

10 CFR 712, "Human Reliability Program." January 1, 2006.

10 CFR 860, "Trespassing on Department of Energy Property." January 1, 2006.

10 CFR 1047, "Limited Arrest Authority and Use of Force by Protective Force Officers." January 1, 2006.

10 CFR 1049, "Limited Arrest Authority and Use of Force by Protective Force Officers of the Strategic Petroleum Reserve." January 1, 2006.

41 CFR 101, "Federal Property Management Regulations Systems." July 1, 2005.

48 CFR 952.204-2, "Security Requirements." October 1, 2005.

Executive Order 12333, "United States Intelligence Activities." December 4, 1981.

Executive Order 12958, "Classified National Security Information." April 17, 1995.

Executive Order 12958, "Classified National Security Information," as amended by Executive Order 13292. March 25, 2003.

U.S. Department of Energy. *Criticality Safety Reference Guide.* March 2006.

U.S. Department of Energy. DOE Manual 231.1-2, Occurrence Reporting and Processing of Operations Information. August 19, 2003.

U.S. Department of Energy. DOE Manual 470.4-1, *Safeguards and Security Program Planning and Management*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-2, *Physical Protection*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-3, *Protective Force*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-4, *Information Security*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-5, *Personnel Security*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-6, *Nuclear Material Control and Accountability*. August 26, 2005.

U.S. Department of Energy. DOE Manual 470.4-7, *Safeguards and Security Program References*. August 26, 2005.

U.S. Department of Energy. DOE Manual 471.2-2, *Classified Information Security Systems Manual*. August 3, 1999.

U.S. Department of Energy. DOE Manual 475.1-1A, *Identifying Classified Information*. February 26, 2001.

U.S. Department of Energy. DOE-NE-STD-1004-92, *Root Cause Analysis Guidance Document.* February 1992.

U.S. Department of Energy. DOE Order 151.1C, *Comprehensive Emergency Management System*. November 2, 2005.

U.S. Department of Energy. DOE Order 200.1, *Information Management Program*. September 30, 1996.

U.S. Department of Energy. DOE Order 231.1A, Chg 1, *Environmental, Safety, and Health Reporting*. June 3, 2004.

U.S. Department of Energy. DOE Order 420.1B, *Facility Safety*. December 22, 2005.

U.S. Department of Energy. DOE Order 470.4, *Safeguards and Security Program.* August 26, 2005.

U.S. Department of Energy. DOE Order 5639.8A, *Security of Foreign Intelligence Information and Sensitive Compartmented Information Facilities*. July 23, 1993.

U.S. Department of Energy. DOE Policy 141.2, *Public Participation and Community Relations*. May 2, 2003.

U.S. Department of Energy. DOE-STD-1070-94, *Guidelines for Evaluation of Nuclear Facility Training Programs*. June 1994.

U.S. Department of Energy. DOE-STD-3006-2000, *Planning and Conduct of Operational Readiness Reviews*. June 2000.

U.S. Department of Energy. DOE-STD-7501-99, *The DOE Corporate Lessons Learned Program*. December 1999.

U.S. Department of Energy. *Radiation Protection Reference Guide.* September 2005.

U.S. Department of Energy. *Technical Program Manager Reference Guide.* September 2005.

Wikipedia. *Felony.* http://en.wikipedia.org/wiki/felony.

# Safeguards and Security Qualification Standard Reference Guide

SEPTEMBER 2006